User Guide

hp StorageWorks Embedded Web Server

Product Version: FW v06.xx/HAFM SW v08.02.00

Third Edition (July 2004)

Part Number: AA–RTDRC–TE/623–000006–001

This guide describes the Embedded Web Server (EWS) and its features. It tells you how to use EWS to configure, operate, and monitor Storage Area Networks (SANs).

Printed in the U.S.A.

Embedded Web Server User Guide
Third Edition (July 2004)
Part Number: AA–RTDRC–TE/623–000006–001

Contents

Figures

Tables

About This Guide

This user guide provides information to help you:

- Use the Embedded Web Server (EWS) to configure and manage the following HP StorageWorks products:
  - Director 2/64
  - Director 2/140
  - Edge Switch 2/12
  - Edge Switch 2/16
  - Edge Switch 2/24
  - Edge Switch 2/32
- Use the Embedded Web Server to monitor Storage Area Networks (SANs).

This chapter includes the following topics:

Overview

This section covers the following topics:

Intended Audience

This book is intended for use by data center administrators, LAN administrators, operations personnel, and customer support personnel who administer user access to this application and monitor and manage product operation.

Related Documentation

For a list of corresponding documentation, see the Related Documents section of the Release Notes that came with the product.

For the latest information, documentation, and firmware releases, please visit the following StorageWorks web site:

http://h18006.www1.hp.com/storage/saninfrastructure.html

For information about Fibre Channel standards, visit the Fibre Channel Association web site, located at http://www.fibrechannel.org.

Conventions

Conventions consist of the following:

- Document Conventions
- Text Symbols
- Equipment Symbols

Document Conventions

This document follows the conventions in Table 1.

Table 1: Document Conventions

Convention	Element
Blue text: Figure 1	Cross-reference links
Bold	Menu items, buttons, and key, tab, and box names
Italics	Text emphasis and document titles in body text
`Monospace font`	User input, commands, code, file and directory names, and system responses (output and messages)
`Monospace, italic font`	Command-line and code variables
Blue underlined sans serif font text (http://www.hp.com)	Web site addresses

Text Symbols

The following symbols may be found in the text of this guide. They have the following meanings:

WARNING: Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or death.

Caution: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or data.

Tip: Text in a tip provides additional help to readers by providing nonessential or optional techniques, procedures, or shortcuts.

Note: Text set off in this manner presents commentary, sidelights, or interesting points of information.

Equipment Symbols

The following equipment symbols may be found on hardware for which this guide pertains. They have the following meanings:

Any enclosed surface or area of the equipment marked with these symbols indicates the presence of electrical shock hazards. Enclosed area contains no operator serviceable parts.

WARNING: To reduce the risk of personal injury from electrical shock hazards, do not open this enclosure.

Any RJ-45 receptacle marked with these symbols indicates a network interface connection.

WARNING: To reduce the risk of electrical shock, fire, or damage to the equipment, do not plug telephone or telecommunications connectors into this receptacle.

Any surface or area of the equipment marked with these symbols indicates the presence of a hot surface or hot component. Contact with this surface could result in injury.

WARNING: To reduce the risk of personal injury from a hot component, allow the surface to cool before touching.

Power supplies or systems marked with these symbols indicate the presence of multiple sources of power.

WARNING: To reduce the risk of personal injury from electrical shock, remove all power cords to completely disconnect power from the power supplies and systems.

Any product or assembly marked with these symbols indicates that the component exceeds the recommended weight for one individual to handle safely.

WARNING: To reduce the risk of personal injury or damage to the equipment, observe local occupational health and safety requirements and guidelines for manually handling material.

Rack Stability

Rack stability protects personnel and equipment.

WARNING: To reduce the risk of personal injury or damage to the equipment, be sure that:

- The leveling jacks are extended to the floor.
- The full weight of the rack rests on the leveling jacks.
- In single rack installations, the stabilizing feet are attached to the rack.
- In multiple rack installations, the racks are coupled.
- Only one rack component is extended at any time. A rack may become unstable if more than one rack component is extended for any reason.

Getting Help

If you still have a question after reading this guide, contact an HP authorized service provider or access our web site: http://www.hp.com.

HP Technical Support

Telephone numbers for worldwide technical support are listed on the following HP web site: http://www.hp.com/support/. From this web site, select the country of origin.

Note: For continuous quality improvement, calls may be recorded or monitored.

Be sure to have the following information available before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

HP Storage Web Site

The HP web site has the latest information on this product, as well as the latest drivers. Access storage at: http://www.hp.com/country/us/eng/prodserv/storage.html. From this web site, select the appropriate product or solution.

HP Authorized Reseller

For the name of your nearest HP authorized reseller:

- In the United States, call 1-800-345-1518
- In Canada, call 1-800-263-5868
- Elsewhere, see the HP web site for locations and telephone numbers: http://www.hp.com.

Introduction

1

This chapter provides an overview of the EWS and describes its user interface. This chapter includes the following topics:

Overview

The Embedded Web Server (EWS) is a web-based graphical user interface (GUI), based on HTML, that enables the user to administer products, monitor products and ports, and perform tasks to manage a simple Storage Area Network (SAN). You can also use EWS to perform troubleshooting tasks and upgrade product firmware.

With product firmware 04.00.00 (or later) installed, administrators or operators with a browser-capable PC and an Internet connection can monitor and manage the product through the EWS interface.

The EWS interface supports product configuration, statistics monitoring, and basic operation. The EWS interface neither replaces nor offers all of the management capability of the High Availability Fabric Manager (HAFM) and its Product Manager applications (for example, the EWS interface does not support all product maintenance functions).

In addition, EWS provides hyperlink access to other products in a fabric, which means those products can also be managed.

Using EWS to Perform Tasks

Users can perform the following tasks using EWS:

- Display the properties and operational status of the product, FRUs, and Fibre Channel ports; display product operating parameters; and display fabric parameters.
- Configure the director or edge switch, including:
  - Fibre Channel port parameters, port types, and data transmission speeds.
  - Product identification, date and time, operating domain parameters, fabric parameters, and network addresses.
  - Parameters for product management through Simple Network Management Protocol (SNMP), the Command Line Interface (CLI), the Open System Management Server (OSMS) feature, or the Fibre Connection (FICON) Management Server (FMS) feature.

Note: The Edge Switch 2/24 does not support out-of-band management through FMS. However, the Edge Switch 2/24 does support transmission of FICON frames.

  - Zones and zone sets.
  - User rights (administrator and operator).
  - Port binding, switch binding, fabric binding, and Enterprise Fabric Management.er rights (administrator and operator).
- Monitor ports and port statistics and display the event log and node list.
- Perform product operations and maintenance tasks, including:
  - Enable unit beaconing, turn off the system error light, set the product online or offline, and perform a configuration reset.
  - Enable port beaconing, perform port diagnostics, and reset ports.
  - Retrieve dump files and retrieve product information files.
  - Install optional feature keys.
  - Configure product Internet Protocol (IP) addresses, names, and SNMP settings.
  - Install new versions of product firmware.
  - Manage user access to features.

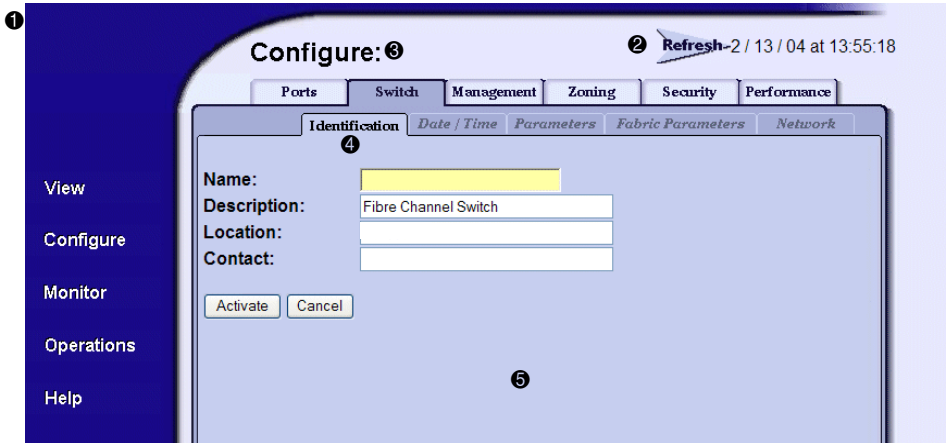
- Control product ports on an individual basis.
- Troubleshoot problems using event log and error status indicators. Administrators and operators can access real-time information about the product and fabric.

The EWS interface can be opened from a standard web browser running Netscape Navigator 4.6 or higher or Microsoft® Internet Explorer 4.0 or higher. At the web browser, the user enters the IP address of the product as the Internet uniform resource locator (URL). When prompted at a login screen, the user enters a user name and password.

Note: The default user name is **Administrator** and the default password is **password.** The user name and password are case-sensitive.

Viewing the User Interface

When the EWS interface opens, the default display is the **View** page. Figure 1 shows an example EWS view with labels for the various parts of the image. This example shows the **Configure > Switch > Identification** screen for the Edge Switch 2/24. For other products, the corresponding page looks very similar.



❶ Navigation Panel
❷ Refresh Icon
❸ Page View
❹ Tabs
❺ Tab View

Figure 1: Example Embedded Web Server page for Edge Switch 2/24

As shown in Figure 1, particular terms are used when describing the EWS interface:

- **Navigation panel** — At the left of the screen is a menu of the various primary views available on the screen. The navigation panel options include:
  - **View** — At the **View** page, the **Director** or **Switch** (default), **Port Properties**, **FRU Properties**, **Unit Properties**, **Operating Parameters**, and **Fabric** task selection tabs display.
  - **Configure** — At the **Configure** page, the **Ports** (default), **Director** or **Switch**, **Management**, **Zoning**, and **User Rights** task selection tabs display.
  - **Monitor** — At the **Monitor** page, the **Port List** (default), **Port Stats**, **Log**, and **Node List** task selection tabs display.

  - — **Operations** — At the **Operations** page, the **Director** or **Switch** (default), **Port**, **Maintenance**, and **Feature Installation** task selection tabs display.
  - — **Help** — The **Help** option opens online user documentation that supports the EWS interface. This manual supplements the online help that is included with the EWS interface.

- **Page** — Describes the entire screen except the navigation panel. When you choose an item from the navigation panel, the corresponding page view displays. For example, choose **Configure** from the navigation panel to view the **Configure** page.
- **Tab** — Describes a label for a viewing option on a page, such as the **Switch** and **Identification** tabs shown in Figure 1. Task selection tabs display at the top of the page. The task selection tabs allow users to perform director- or switch-specific tasks.
- **Tab view** — Describes the fields, buttons, and labels that display when you click a tab. The tab view contains the information you are trying to access and activities that you can complete.
- **Date and Time** — Specifies the time when the information shown on the page view was last updated.

Benefits

The EWS interface provides the following benefits:

- Enables a single product to be managed from a single point of access.
- Allows an administrator to manage a product from any location (such as their office, a raised floor area, or a conference room) within the company's public/private networks.
- Enables an administrator to view the most current information about a product upon accessing the product.

  (This easy access provides a single point of product administration that is not limited to the location of an application or special hardware.)
- Protects the authorized rights of users to perform tasks through roles defined as operators and administrators.

  (This protection enables companies to decide who should perform everyday tasks, such as monitoring product status, and sensitive tasks, such as installing firmware updates. This flexible approach enables companies to define roles within their organization while providing a level of security against unauthorized access.)
- Enables users to simply start a web browser, enter the network address of the product, and log in to start using EWS.

  (No additional installation is required. EWS is ready and available to perform administration tasks once the hardware is installed and connected to the Ethernet network.)
- Allows users to utilize a familiar web browser-based graphical user interface that uses standard web browser applications for access.
- Allows users to obtain assistance in performing tasks through online help.

Key Terms

This section provides key terms that will help you perform tasks, especially tasks such as zoning.

Fabric

Entity that interconnects N_Ports and is capable of routing (switching) Fibre Channel frames using the destination ID information in the Fibre Channel frame header accompanying the frames.

Storage Area Network (SAN)

A high-performance data communications environment that interconnects computing and storage resources so that the resources can be effectively shared and consolidated.

Zone (Zoning)

A zone is a group of devices or zone members in a SAN that can communicate and access each other. Communication is only allowed between devices in the same zone. A device can be in multiple zones so that shared resources can be accessed by many devices. Because SANs connect many types of devices that may carry different protocols, separating an entire fabric into zones can control access between specific devices. Zone (or zoning) is an efficient method of managing, partitioning, and controlling access to SAN devices. Zoning maximizes resources while maintaining data security and enabling heterogeneous systems and products to operate in the same SAN.

Zone Member

Specification (definition) of a device that belongs to a zone. A zone member can be identified by the port number of the device to which it is attached or by its device or host bus adapter or World Wide Name (WWN). In multiswitch fabrics, identification of end-devices and nodes by WWN is preferable.

Zone Set

A zone set is composed of one or more zones. When a zone set is activated, all zones in the set are activated at the same time. Only one zone set can be active in the fabric at one time, and that zone set is referred to as the active zone set.

Suggested Reading

A book that can help you to prepare to install products and configure a SAN is the *HP StorageWorks SAN High Availability Planning Guide.* You can obtain this book from the Hewlett-Packard web site (http://www.hp.com) or from the CD shipped with the Hewlett-Packard product you purchased.

Another publication you may want to read is *Compaq StorageWorks SAN Switch Zoning Reference Guide*, which is a white paper on zoning fundamentals. It is available online from the Hewlett-Packard web site (http://www.hp.com).

Where to Start

Depending upon whether the Hewlett-Packard product you purchased has already been installed, you may need to go to a specific chapter. If the product has not been installed, you should start at “Configuring the Product” on page 29.

If the product was installed, then many of the configuration tasks were probably already completed. In that case, you may need to configure a zone. Configuring (including adding, deleting, and changing) zones is described in “Configuring Zones” on page 81

If the products have been configured and you have a functioning SAN, then you most likely will be interested in performing system administration tasks. Those tasks are described in “Viewing Product and Fabric Data” on page 99, “Monitoring Products” on page 117, and “Operating and Managing Products and Parts” on page 135.

If you need to perform troubleshooting, then you will want to review “Monitoring Products” on page 117 and “Operating and Managing Products and Parts” on page 135.

Starting EWS

Open the EWS interface as follows:

1. Ensure the workstation (or device you use to launch the web browser) and the Ethernet LAN segment containing the product, such as Edge Switch 2/24, are attached and connected through the Internet.

Note: You must be able to make a connection between the web browser and the product in order to log in to the product.

---

2. Launch the web browser application (such as Netscape Navigator, version 4.6 or higher, or Microsoft Internet Explorer, version 4.0 or higher).
3. At the web browser, enter the IP address of the product as the Internet uniform resource locator (URL) such as `http://10.1.1.11`.

Note: If the product has not been installed, refer to the product's installation and service manual for the appropriate IP address, login ID, and password that is initially used when you install and configure the product.

After a connection is made between the web browser and the product, the logon dialog box displays as shown in Figure 2.

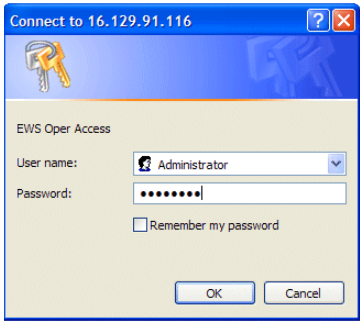


Figure 2: Logon dialog box

4. Type the user name and password. The EWS interface opens with the **View** page displayed, as shown in Figure 3.

Note: The default user name is available from the installation and service guide that was shipped with the product. The user name and password are case-sensitive. Also, during installation, the default values may have been changed. If defaults have changed, contact your system administrator for the valid user names and passwords.

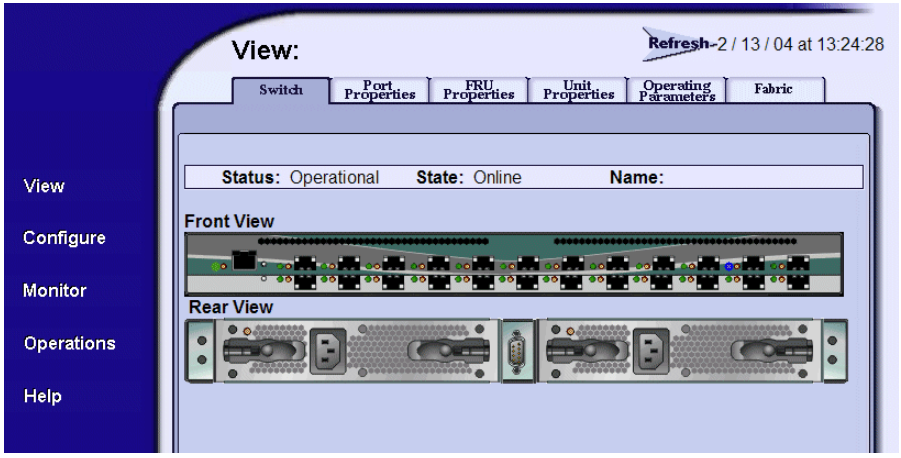


Figure 3: View Page

Configuring the Product

2

This chapter describes how to configure an HP product using the EWS interface. These procedures can be used to configure a product after installation and as changes are needed. You can use the tabs of the **Configure** page to configure the following aspects of a director or edge switch:

Factory Default Values

HP products on a SAN have preset, default configuration values that were set in the factory. The items that have factory-set default values are:

- Passwords (customer and maintenance-level)
- Internet Protocol (IP) address
- Subnet mask
- Gateway address

The specific default values associated with a particular HP product are documented in the installation and service manual for the product.

Configuring Ports

Perform procedures in this section to configure names and operating characteristics for Fibre Channel ports. To configure one or more ports:

1. If you are going to change the **Speed** parameter on a Director 2/64, set the product offline as follows:
   a. Choose **Operations** from the navigation panel. The **Operations** page displays.
   b. Click the **Online State** tab, then click **Set Offline**. The following message displays: `Your operations changes have been successfully activated`.
2. At the EWS screen, choose **Configure** from the navigation panel. The **Configure** page and the **Ports** tab view display (Figure 4).

Note: Because the Director 2/140 has many ports, the listing of ports is divided into separate displays, which are accessed by clicking the hyperlinks **1-31**, **32-63**, **64-95**, **96-127**, and **132-143**. (Ports 128 through 131 are internal ports and not available for external connections.) If you make any changes to a particular list of ports, click **Activate** before selecting another list of ports. If you do not click **Activate**, changes are not implemented on the director.

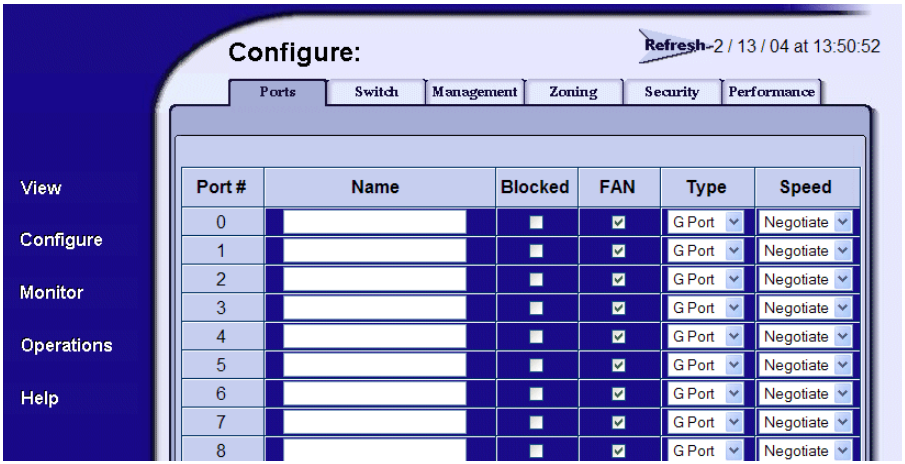


Figure 4: Configure Ports tab view

a. For each port to be configured, type a port name of 24 alphanumeric characters or less in the associated **Name** field.

Note: When naming ports, you may want to name each port based on the device attached to the port. For example, if the port is attached to an e-mail server, you might name the port `email1 server port 2`. The important point is to relate the name of the port to the device that is attached to the port.

---

b. Click a check box in the **Blocked** column to block or unblock a port (default is unblocked). A check mark in the box indicates a port is blocked. Blocking a port prevents the attached devices or HP products in the fabric from communicating. A blocked port continuously transmits the offline sequence (OLS).

c. Click the check box in the **FAN** column to enable or disable the fabric address notification (FAN) feature (default is enabled). (The **FAN** column is available only on the Edge Switch 2/24.) A check mark in the box indicates FAN is enabled. When the feature is enabled, the port transmits a FAN frame after loop initialization to verify that Fibre Channel Arbitrated Loop (FC-AL) devices are still logged in. It is recommended this option be enabled for ports configured for loop operation.

d. Click a check box in the **10—100 km** column to define extended distance buffering. (This column is not available on the Edge Switch 2/24.) A check mark in the box indicates extended distance buffering is enabled.

You can enable extended distance for a port even if it is not an extended distance port. However, enabling extended distance buffering for a port disables the ability of the port to send broadcast traffic. When you choose this option, the port can support up to 60 buffer-to-buffer credits (BB_Credits) to handle link distances up to 100 km. This enables the port to process 2K frames from attached devices. If this option is not enabled, the port uses the BB_Credit value.

Note: If a device is connected and logged in to the fabric when extended distance is enabled or disabled on the corresponding port, the HP product sends OLS for 5 milliseconds to force the device to log in again and obtain the new BB_Credit value set for the port.

---

e. Choose from the drop-down list in the **Type** column to configure the port type. Available selections are:

   — **G_Port** — Generic port.

   — **F_Port** — Fabric port.

   — **E_Port** — Expansion port.

   — **GX_Port** — Generic mixed port. Use this selection to configure a port as a generic loop port (GL_Port). The port automatically negotiates any connection type (Edge Switch 2/24 only).

   — **FX_Port** — Fabric mixed port. Use this selection to configure a port as a fabric loop port (FL_Port). The port automatically negotiates F_Port and FL_Port connections only (Edge Switch 2/24 only).

f. Choose from the drop-down list in the **Speed** column to configure the port transmission rate. Available selections are:

   — **Negotiate** — Auto-negotiate between 1.0625 and 2.125 gigabits per second (Gb/s) operation. This is valid only on products that are capable of 2 Gbs operation.

   — **1 Gb/sec** — 1.0625 Gb/s operation.

   — **2 Gb/sec** — 2.125 Gb/s operation.

3. Click **Activate** to save and activate the changes. The following message displays: `Your changes to the port configuration have been successfully activated`.

4. If the product is offline, set the product online as follows:
   a. Choose **Operations** from the navigation panel. The **Operations** page displays.
   b. Click the **Online State** tab, then click **Set Online**. The following message message displays: `Your operations changes have been successfully activated`.

Configuring Product Identification

Perform this procedure to configure the HP product's name, description, location, and contact person. The **Name**, **Location**, and **Contact** variables configured here correspond respectively to the variables used by SNMP management workstations when obtaining data from managed edge switches or directors. To configure identification:

1. Choose **Configure** from the navigation panel. Choose the **Switch** or **Director** tab, as appropriate. The **Switch** or **Director** tab displays with the **Identification** tab view (Figure 5).

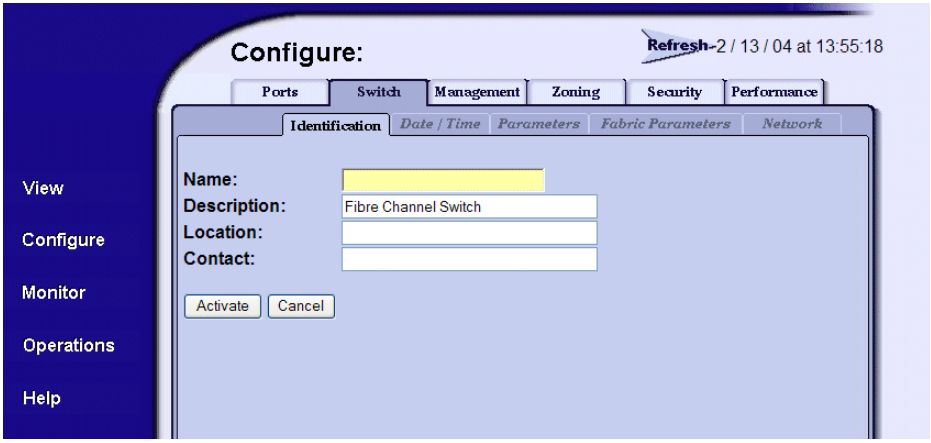


Figure 5: Configure product Identification tab view

a. Type a name of 24 alphanumeric characters or less in the **Name** field. Each product should be configured with a unique name.

   If the product is installed on a public LAN, it is recommended that the name reflect the product's Ethernet network domain name system (DNS) host name. For example, if the DNS host name is `edgeswitch224.hp.com`, the name entered in this dialog box should be `edgeswitch224`.

Note: Spaces are allowed in the **Name** field.

---

b. Type a product description of 255 alphanumeric characters or less in the **Description** field.

c. Type the product's physical location (255 alphanumeric characters or less) in the **Location** field.

d. Type the name of a contact person (255 alphanumeric characters or less) in the **Contact** field.

2. Click **Activate** to save and activate the changes. The following message displays: `Your changes to the identification configuration have been successfully activated`.

Configuring Date and Time

Perform this procedure to configure the effective date and time for the product. To set the date and time:

1. Choose **Configure** from the navigation panel. Choose the **Switch** or **Director** tab, as appropriate. Click the **Date/Time** tab to display the **Date/Time** tab view (Figure 6).

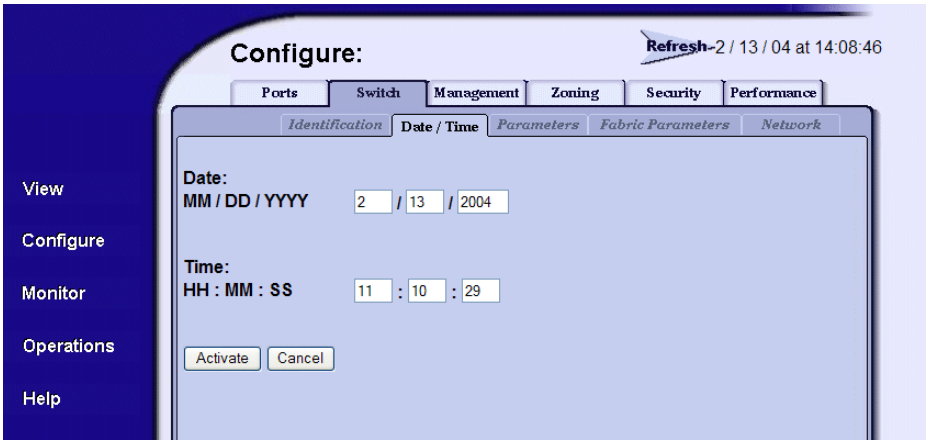


Figure 6: Configure Date and Time tab view

   a. Click the **Date** fields that require change, and type numbers in the following ranges:
      - Month (**MM**): `01` through `12`.
      - Day (**DD**): `01` through `31`.
      - Year (**YYYY**): greater than `1980`.
   b. Click the **Time** fields that require change, and type numbers in the following ranges:
      - Hour (**HH**): `00` through `23`.
      - Minute (**MM**): `00` through `59`.
      - Second (**SS**): `00` through `59`.
2. Click **Activate** to save and activate the changes. The following message displays: `Your changes to the date/time configuration have been successfully activated.`

Configuring Operating Parameters

Perform this procedure to configure the product's preferred domain ID, insistent domain ID, rerouting delay, and domain registered state change notifications (RSCN). The product must be set offline to configure the preferred domain ID. To configure parameters:

1. If you are going to set the preferred domain ID, set the product offline as follows:
   a. Choose **Operations** from the navigation panel. The **Operations** page displays.
   b. Click the **Online State** tab, then click **Set Offline**. The following message displays: `Your operations changes have been successfully activated`.
2. Choose **Configure** from the navigation panel. The **Configure** page displays.
3. Click the **Switch** or **Director** tab, as appropriate. Click the **Parameters** tab to display the **Parameters** tab view (Figure 7).

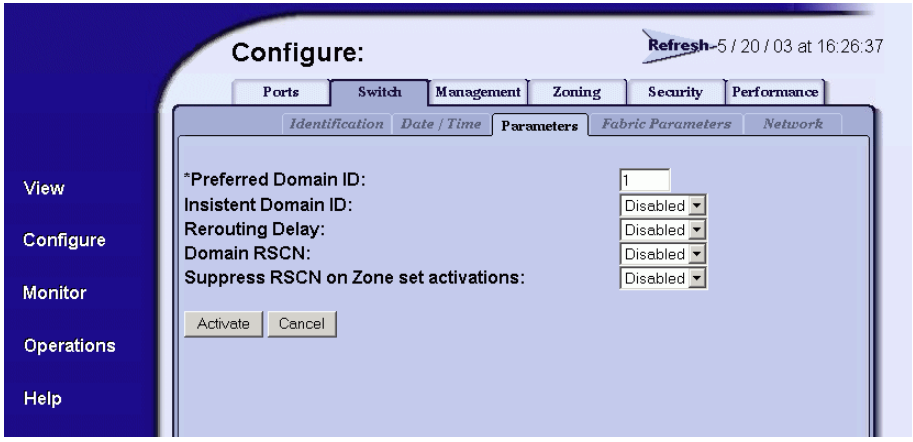


Figure 7: Configure product Parameters tab view

   a. At the **Preferred Domain ID** field, type a value of `1` through `31`. The domain ID uniquely identifies each product in a fabric.

Note: If the product is attached to a fabric element, the product and element must have unique domain IDs. If the values are not unique, the E_Port connection to the element cannot carry traffic and the product cannot communicate with the fabric.

---

b. At the **Insistent Domain ID** field, choose **Enabled** or **Disabled**. When this parameter is enabled, the domain ID configured in the **Preferred Domain ID** field becomes the active domain identification when the fabric initializes. (The Insistent Domain ID is automatically enabled if the SANtegrity Binding feature is installed.)

Note: If Enterprise Fabric Mode (an optional SANtegrity Binding feature) or Fabric Binding is enabled, then Insistent Domain ID must be enabled.

---

c. At the **Rerouting Delay** field, choose **Enabled** or **Disabled**. When this parameter is enabled, traffic is delayed through the fabric by the specified error detect time out value (E_D_TOV). This delay ensures Fibre Channel frames are delivered to their destination in order, even if a change to the fabric topology creates a new (shorter) transmission path. This parameter is only applicable if the product is being configured in a multiswitch fabric.

Note: If Enterprise Fabric Mode (an optional SANtegrity Binding feature) is enabled, then Rerouting Delay must be enabled.

---

d. At the **Domain RSCN** field, choose **Enabled** or **Disabled**. When this parameter is enabled, messages can be sent between end devices in a fabric to provide additional connection information to host bus adapters (HBA) and storage devices. Consult with your HBA and storage device vendor to determine if enabling Domain RSCNs will cause problems with your HBA or storage products.

Note: If Enterprise Fabric Mode (an optional SANtegrity Binding feature) is enabled, then Domain RSCN must be enabled.

---

e. At the **Suppress RSCN on Zone Set Activations** field, choose **Enabled** or **Disabled**. When this parameter is enabled, RSCN messages are prohibited from being sent to ports on the switch following any change to the fabric's active zone set. Consult with your HBA and storage device vendor to determine if enabling this parameter will cause problems with your HBA or storage products.

Note: Some older versions of EWS may show the **Zoning Configuration Change RSCNs** field for this item. The functionality is the same.

f. If you are configuring parameters for the Director 2/64, a **Switch Speed** field is displayed. Choose **1 Gb/sec** or **2 Gb/sec**. These options specify the speed used on the switch. This field is valid only for the Director 2/64, which is able to run at both speeds.

4. Click **Activate** to save and activate the changes. The following message displays: `Your changes to the operating parameters configuration have been successfully activated`.
5. If fabric parameters require configuration, go to "Configuring Fabric Parameters" on page 41. If the configuration is complete, set the product online as follows:
   a. Choose **Operations** from the navigation panel. The **Operations** page displays.
   b. Click the **Online State** tab, then click **Set Online**. The following message displays: `Your operations changes have been successfully activated`.

Configuring Fabric Parameters

Perform this procedure to configure the fabric operating parameters, including resource allocation time out value (R_A_TOV), E_D_TOV, switch priority, interop mode, and buffer-to-buffer credit. The product must be set offline.

Note: An Edge Switch 2/12 cannot participate in a fabric unless the Fabric Capable feature is enabled. For more information, see the *Edge Switch 2/12 Installation Guide*.

To configure parameters:

1. If product is online, set the product offline as follows:
   a. Choose **Operations** from the navigation panel. The **Operations** page displays.
   b. Click the **Online State** tab, then click **Set Offline**. The following message displays: `Your operations changes have been successfully activated`.
2. Choose **Configure** from the navigation panel.
3. Click the **Switch** or **Director** tab (as appropriate), then click the **Fabric Parameters** tab. The **Fabric Parameters** tab view displays (Figure 8).

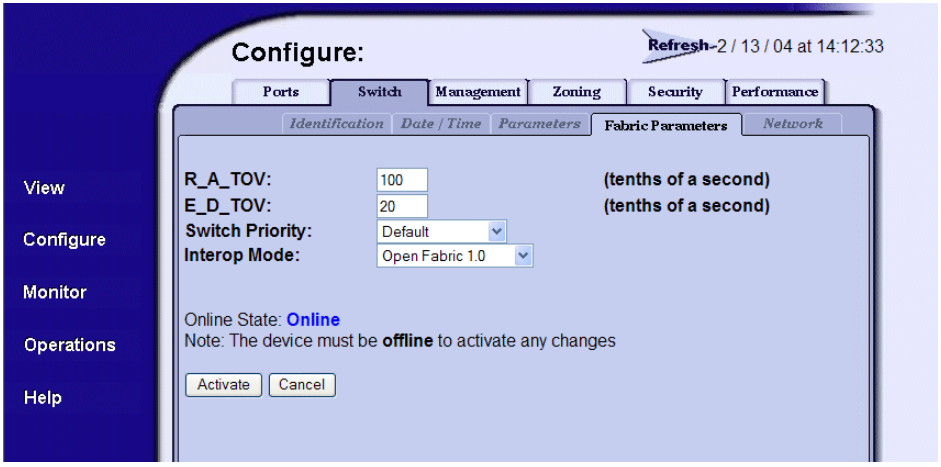


Figure 8: Fabric Parameters tab view

a. At the BB_Credit field, type a value between `1` and `60`. (This field is not available for the Edge Switch 2/24.) Configure the product to support buffer-to-buffer credit (BB_Credit) from 1 through 60. This is the value used for all ports, except those configured for extended distance buffering (10—100 km). The default value is 16. For a description of the buffer-to-buffer credit, refer to industry specification, *Fibre Channel Physical and Signaling Interface*.

b. At the **R_A_TOV** field, type a value between `10` through `1200` tenths of a second (1 through 120 seconds). (The R_A_TOV value must be greater than the E_D_TOV value.)

Note: If the product is attached to a fabric element, the product and element must be set to the same R_A_TOV value. If the values are not identical, the E_Port connection to the element fails and the product cannot communicate with the fabric.

---

c. At the **E_D_TOV** field, type a value between `2` through `600` tenths of a second (0.2 through 60 seconds). (The E_D_TOV value must be less than the R_A_TOV value.)

Note: If the product is attached to a fabric element, the product and fabric element must be set to the same E_D_TOV value. If the values are not identical, the E_Port connection to the element fails and the product cannot communicate with the fabric.

d. Choose from the **Switch Priority** drop-down list to set the product priority. Available selections are **Default**, **Principal**, and **Never Principal**. The default setting is **Default**.

   This value designates the fabric's principal switch. The principal switch is assigned a priority of **1** and controls the allocation and distribution of domain IDs for all fabric elements (including itself).

   Principal is the highest priority setting, **Default** is the next highest, and **Never Principal** is the lowest priority setting. The setting **Never Principal** means the switch is incapable of becoming a principal switch. If all switches are set to **Principal** or **Default**, the switch with the highest priority and the lowest World Wide Name (WWN) becomes the principal switch.

   At least one switch in a fabric must be set as **Principal** or **Default**. If all switches are set to **Never Principal**, all interswitch links (ISLs) will segment, causing a failure of connectivity.

e. Choose from the **Interop Mode** drop-down list to set the product operating mode. This option does not display if the operation mode is S/390. (S/390 mode is not supported with the Edge Switch 2/24.)

Note: The operation mode parameter in the EWS interface is equivalent to the management style parameter in the HAFM interface. The S/390 mode used for the EWS interface is equivalent to the FICON management style in the HAFM.

   This setting only affects the mode used to manage the product; it does not affect port operation. Available selections are:

   — **Homogenous Fabric** — Choose this option if the product is fabric-attached only to other HP directors or switches operating in Homogenous Fabric mode.

— **Open Fabric 1.0** — Choose this option for managing heterogeneous fabrics and if the product is fabric-attached to HP directors or switches and open-fabric compliant switches produced by other original equipment manufacturers (OEMs). This setting is the default.

4. Click **Activate** to save and activate the changes. The following message displays: `Your changes to the fabric parameters configuration have been successfully activated`.
5. Set the product online as follows:
   a. Choose **Operations** from the navigation panel. The **Operations** page opens.
   b. Click the **Online State** tab, then click **Set Online**. The following message displays: `Your operations changes have been successfully activated`.

Configuring Network Information

Verify the type of LAN installation with the customer's network administrator. If one HP product is installed on a dedicated LAN, network information (IP address, subnet mask, and gateway address) does not require change.

If multiple HP products are installed or a public LAN segment is used, network information must be changed to conform to the customer's LAN addressing scheme.

Perform the following steps to change a product's IP address, subnet mask, or gateway address.

1. Choose **Configure** from the navigation panel.
2. Click the **Switch** or **Director** tab, then click the **Network** tab to display the **Network** tab view (Figure 9).

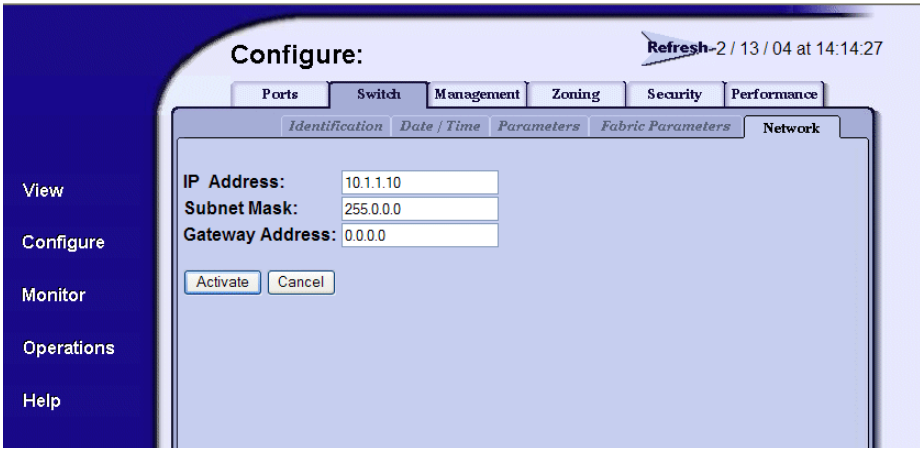


Figure 9: Configuring network parameters tab view

   a. At the **IP Address** field, type the new value specified by the customer's network administrator (default is **10.1.1.10**).
   b. At the **Subnet Mask** field, type the new value specified by the customer's network administrator (default is **255.0.0.0**).
   c. At the **Gateway Address** field, type the new value specified by the customer's network administrator (default is **0.0.0.0**).
3. Click **Activate** to save and activate the changes. The following message box displays (Figure 10).

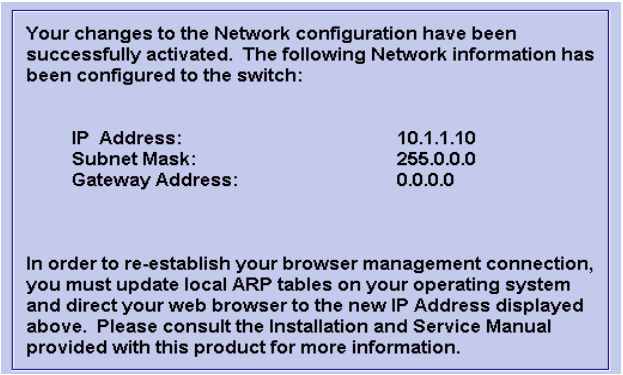


Figure 10: Network information message box

4. Update the address resolution protocol (ARP) table for the browser PC. Delete the product's **old** IP address from the ARP table using the process that is appropriate for the operating system (OS) in use by the system.
5. At the PC, launch the browser application (Netscape Navigator or Internet Explorer).
6. At the browser, enter the product's **new** IP address as the Internet URL. The **Enter Network Password** dialog box displays.
7. Type the user name and password.

Note: The default user name is **Administrator** and the default password is **password.** The user name and password are case-sensitive.

---

8. Click **OK**. The EWS interface opens with the **View** page open and the **Switch** or **Director** page displayed.

Configuring SNMP

Note: The ability of the **SNMP** tab to configure SNMP depends on whether this licensed feature is active on the product.

Perform this procedure to enable the SNMP agent, configure community names, write authorizations, network addresses, and user datagram protocol (UDP) port numbers for up to six SNMP trap message recipients. A trap recipient is a management workstation that receives notification (through SNMP) if a switch event occurs. To configure SNMP trap recipients:

1. Choose **Configure** from the navigation panel.
2. Choose the **Management** tab. The **Management** and **SNMP** tab views display (Figure 11).

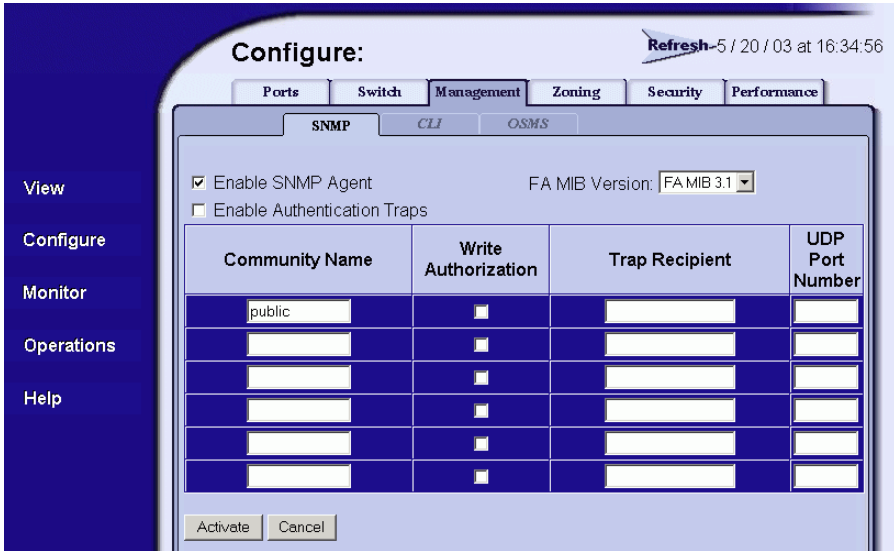


Figure 11: Configure SNMP parameters tab view

a. Click the Enable **SNMP Agent** field to enable SNMP. Clear the check box to disable the SNMP Agent.

b. Click the **Enable Authorization Traps** field to enable authorization trap messages to be sent to SNMP management stations when unauthorized stations try to access SNMP information from the product.

c. Select a Fibre Alliance Management Information Base (FA MIB) version in the **FA MIB Version** field. The options are **FA MIB 3.0** and **FA MIB 3.1**. This should be set to match the level of FA MIB used by the SNMP management stations that access the product.

d. For each trap recipient to be configured, type a community name of 32 alphanumeric characters or less in the **Community Name** field. The community name is incorporated in SNMP trap messages to prevent unauthorized viewing or use.

Note: Spaces are allowed in the **Community Name** field.

e. Click the check box in the **Write Authorization** column to enable or disable write authorization for the trap recipient (default is disabled). A check mark indicates write authorization is enabled. When the feature is enabled, a management workstation user can change **sysContact**, **sysName**, and **sysLocation** SNMP variables.

f. Type the IP address or DNS host name of the trap recipient (SNMP management workstation) in the **Trap Recipient** field in four-byte, dotted-decimal format. It is recommended the IP address be used.

g. The default UDP port number for trap recipients is **162**. Type a decimal. The range for the UDP port number value is 1 to 65535.

3. Click **Activate** to save and activate the changes. The following message displays: `Your changes to the SNMP configuration have been successfully activated`.

Enabling or Disabling the CLI

Perform this procedure to enable or disable the state of the product's command line interface (CLI). To change the CLI state:

1. Choose **Configure** from the navigation panel.
2. Click the **Management** tab and the **CLI** tab. The **CLI** tab view displays (Figure 12).

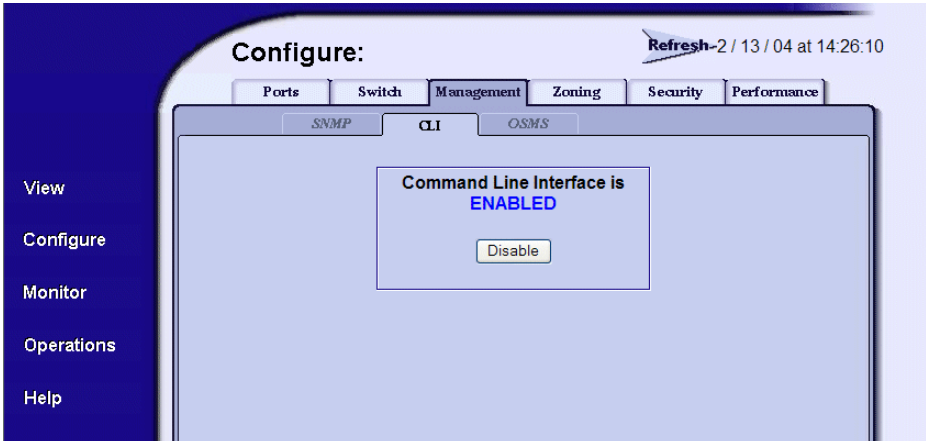


Figure 12: Disabling the CLI

3. Perform one of the following steps as required:
   a. Click **Enable** to activate the CLI. The following message displays: `Your changes to the CLI enable state have been successfully activated.`
   b. Click **Disable** to deactivate the CLI. The following message displays: `Your changes to the CLI enable state have been successfully activated.`

Enabling or Disabling Host Control

Perform this procedure to enable or disable host control of the product through the OSMS.

The OSMS is a keyed feature that allows host control and inband management of the director or switch through a management application that resides on an open-systems interconnection (OSI) device. This device is attached to a director or switch port. The device communicates with the switch or director through Fibre Channel common transport (FC-CT) protocol.

The OSMS feature must be installed to access this control. Refer to "Installing Feature Keys" on page 77 for instructions. If the feature is not installed, the message `Feature not installed` displays. To enable or disable host control:

1. Choose **Configure** from the navigation panel.
2. Choose the **Management** tab and the **OSMS** tab. The **OSMS** tab view displays (Figure 13).

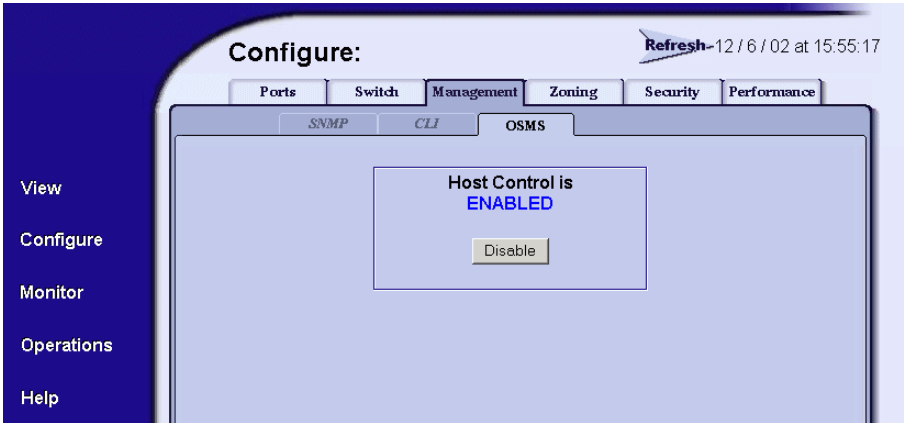


Figure 13: Enabling OSMS host control

3. Perform one of the following steps as required:
   a. Click **Enable** to activate the OSMS host control. The following message displays: `Your changes to the host control enable state have been successfully activated.`
   b. Click **Disable** to deactivate the OSMS host control. The following message displays: `Your changes to the host control enable state have been successfully activated.`

Zoning Tab View

The functionality provided by the **Zoning** tab view is described in “Configuring Zones” on page 81.

Configuring User Rights

EWS has two login IDs, the administrator-level ID and the operator-level ID. These user names and passwords are used to access the EWS interface through the **Enter Network Password** dialog box. (For a listing of user rights availability for the Administrator and Operator, see "User Rights Settings" on page 53.)

The default administrator-level user name is `Administrator` and the default password is `password`. The default operator-level user name is `Operator` and the default password is `password`. All user names and passwords are case-sensitive.

To configure user names and passwords:

1. Choose **Configure** from the navigation panel.
2. Choose the **Security** tab and the **User Rights** tab. The **User Rights** tab view displays (Figure 14) showing the Administrator and Operator user access levels.

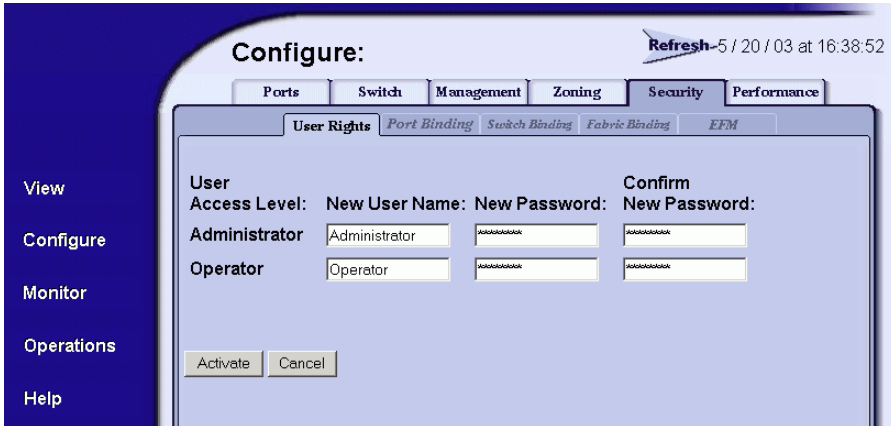


Figure 14: Configuring user IDs

3. For the **Administrator** set of data fields:
   a. Type the administrator user name (as specified by the customer's network administrator) in the **New User Name** field. Use 16 alphanumeric characters or less.
   b. Type the administrator password (as specified by the customer's network administrator) in the **New Password** field. Use 16 alphanumeric characters or less.

c. Type the administrator password again in the **Confirm New Password** field.

4. For the **Operator** set of data fields:
   a. Type the operator user name (as specified by the customer's network administrator) in the **New User Name** field. Use 16 alphanumeric characters or less.
   b. Type the operator password (as specified by the customer's network administrator) in the **New Password** field. Use 16 alphanumeric characters or less.
   c. Type the operator password again in the **Confirm New Password** field.
5. Click **Activate**. The **User Rights** tab redisplays with the message `Your changes to the User Rights configuration have been successfully activated. Login may be required`. The new settings for user name and password are implemented.

Note: In some cases, you may need to log into EWS again to continue using EWS.

User Rights Settings

Table 2 lists the management functions provided by EWS along with the access permissions for each function. If a user lacks the rights to access a specific function, they will receive a login password dialog box indicating the rights (either administrator or operator) required to access the function.

Table 2: User Rights Levels

Functionality	Administrator Rights	Operator Rights
View: Product	Available	Available
View: Port Properties	Available	Available
View: FRU Properties	Available	Available
View: Product Properties	Available	Available
View: Fabric - Products	Available	Available
View: Fabric - Topology	Available	Available
View: Operating Parameters	Available	Available
Configure: Ports	Available	Available

Table 2: User Rights Levels (Continued)

Functionality	Administrator Rights	Operator Rights
Configure: Product Identification	Available	Unavailable
Configure: Product Date/Time	Available	Unavailable
Configure: Product Parameters	Available	Unavailable
Configure: Fabric Parameters	Available	Unavailable
Configure: Product Network	Available	Unavailable
Configure: Management SNMP	Available	Unavailable
Configure: Management CLI	Available	Unavailable
Configure: Management OSMS	Available	Unavailable
Configure: Zone Set	Available	Unavailable
Configure: Zones	Available	Unavailable
Configure: Modify Zone	Available	Unavailable
Configure: Security - Port Binding	Available	Unavailable
Configure: Security - User Rights	Available	Unavailable
Configure: Security - Switch Binding	Available	Unavailable
Configure: Security - Fabric Binding	Available	Unavailable
Configure: Security - EFM	Available	Unavailable
Configure: Performance - Open Trunking	Available	Unavailable
Monitor: Port List	Available	Available
Monitor: Port Stats	Available	Available
Monitor: Logs	Available	Available
Monitor: Node List	Available	Available
Operations: Product Beacon	Available	Available
Operations: Product Online State	Available	Unavailable
Operations: Product Reset Config	Available	Unavailable
Operations: Port Beacon	Available	Available
Operations: Port Reset	Available	Available
Operations: Port Diagnostics	Available	Unavailable

Table 2: User Rights Levels (Continued)

Functionality	Administrator Rights	Operator Rights
Operations: Maintenance Dump Retrieval	Available	Unavailable
Operations: Maintenance Product Info	Available	Unavailable
Operations: Maintenance Firmware Upgrade	Available	Unavailable
Operations: Feature Installation	Available	Unavailable
Help	Available	Available

Binding Ports to Devices

The **Port Binding** tab view enables you to *bind* a specific switch or director port to the WWN of an attached device for exclusive communication.

To configure port binding:

1. Choose **Configure** from the navigation panel.
2. Choose the **Security** tab and the **Port Binding** tab. The **Port Binding** tab view displays (Figure 15).

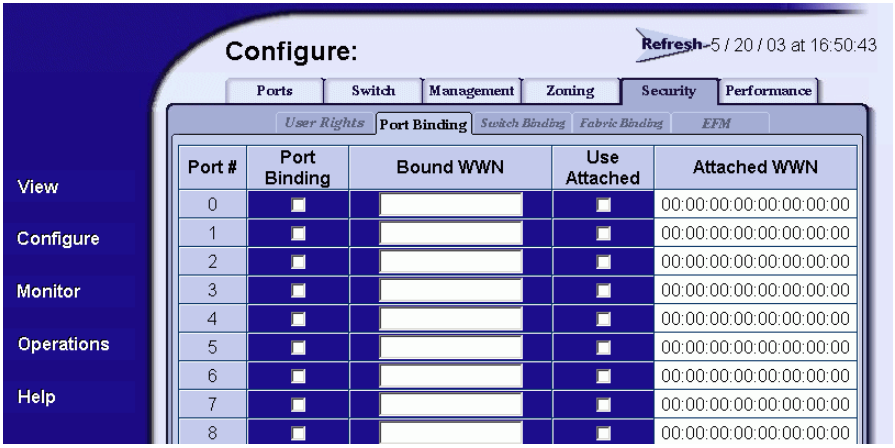


Figure 15: Configuring Port Binding

3. Click the check box in the **Port Binding** column next to the port number to enable port binding for the port.
4. Identify the WWN to which the port is bound using one of the following methods:
   - Enter the WWN to which the port is to bind in the **Bound WWN** column.
   - Click the check box in the **Use Attached** column. This option is valid only if a WWN is present in the **Attached WWN** column for the port. (The **Attached WWN** column indicates the WWN that is currently attached to the port, but is not bound to it.)

Note: If the **Port Binding** check box is checked and a WWN is not specified for binding, no devices can attach to the port.

5. Click the **Activate** button at the bottom of the screen.

Configuring Switch Binding

Switch Binding functionality enables you to identify the devices with which the switch or director can communicate. Switch Binding is available only if the SANtegrity Binding feature is installed.

The **Switch Binding** tab view allows you to enable the product to communicate only with devices that are listed on the Switch Binding Membership List (SBML). Switch Binding restricts connections to only the devices listed on the SBML and allows no other devices to communicate with the switch. When an unauthorized WWN attempts to log in, it is denied a connection and an event is posted to the event log. This provides security in environments that include a large number of devices by ensuring that only the specified set of devices are able to attach to a switch or director.

You can use the **Switch Binding** tab to enable Switch Binding and to create and change the SBML.

Note: Switch Binding can also be enabled by enabling the Enterprise Fabric Mode. For more information, see "Switch Binding and the Enterprise Fabric Mode" on page 72.

Enable, Disable, and Online State Functions

For Switch Binding to function, specific operating parameters and optional features must be enabled. Also, there are specific requirements for disabling these parameters and features:

- Switch Binding can be enabled or disabled whether the product is offline or online.
- Enabling Enterprise Fabric Mode automatically enables Switch Binding.
- You cannot disable Switch Binding if Enterprise Fabric Mode is enabled. However, if Enterprise Fabric Mode is disabled, you can disable Switch Binding.
- If Enterprise Fabric Mode is enabled and the director or switch is online, you cannot disable Switch Binding.
- If Enterprise Fabric Mode is enabled and the director or switch is offline, you can disable Switch Binding, but this also disables Enterprise Fabric Mode.

- WWNs can be added to the SBML without regard to whether Switch Binding is enabled or disabled.
- If the director or switch is online and Switch Binding is not enabled, all nodes and switches attached to the director or switch are automatically added to the SBML.

Enabling and Disabling Switch Binding

Note: Switch Binding can also be enabled by enabling the Enterprise Fabric Mode. For more information, see "Switch Binding and the Enterprise Fabric Mode" on page 72.

To enable or disable Switch Binding:

1. Select **Configure** from the navigation panel.
2. Select the **Security** tab and the **Switch Binding** tab. The **Switch Binding** tab view displays (Figure 16).

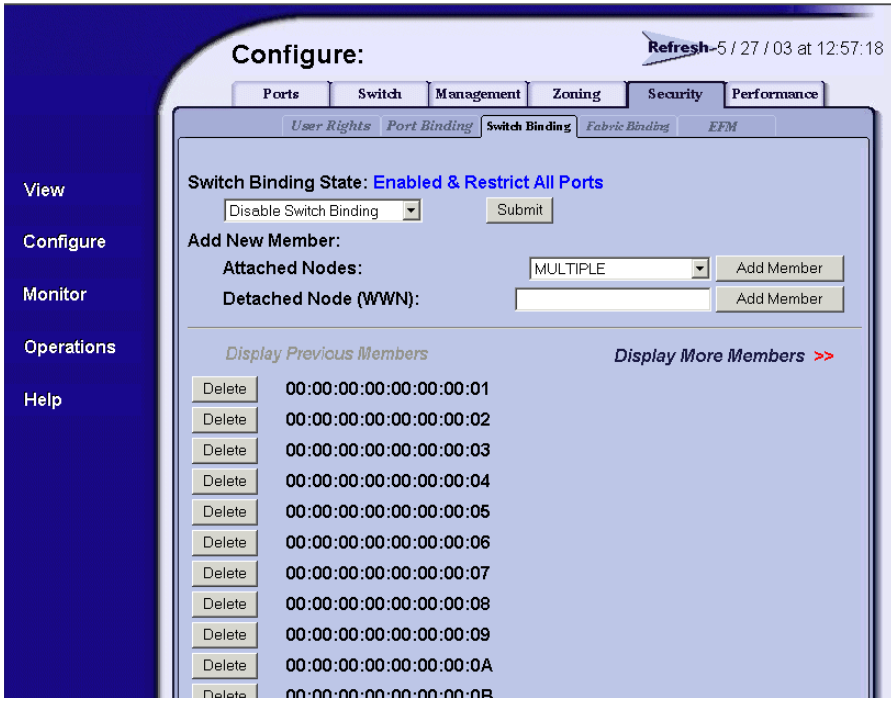


Figure 16: Configuring Switch Binding

3. Enable or disable Switch Binding by selecting one of the following options from the **Switch Binding State** drop-down list. Available selections are:
   - **Enable & Restrict E Ports —** Enables the switch to bind to devices listed on the SBML through E_Ports only.
   - **Enable & Restrict F Ports —** Enables the switch to bind to devices listed on the SBML through F_Ports only.
   - **Enable & Restrict All Ports —** Enables the switch to bind to devices listed on the SBML through all port types.
   - **Disable Switch Binding —** Sets the Switch Binding State to disabled. No restrictions apply as to which devices can attach to this switch. This option is not valid if Enterprise Fabric Mode is enabled.
4. Click the **Submit** button to activate your choice.

Configuring the Switch Binding Membership List

The SBML contains the WWNs of devices that are allowed to communicate with the switch when Switch Binding is enabled. This list is configured using the **Switch Binding** tab.

The contents of the SBML are shown at the bottom of the tab, listed by WWN. The tab can show up to 64 list members. If the list contains more than 64 members, the other list members are shown on subsequent pages. To see the next page of list members, click the **Display More Members** option. To see the previous page of list members, click the **Display Previous Members** option. The message `All Members Displayed` appears on the last page of entries.

Adding a List Member

To add a new member to the SBML, perform the following procedure:

1. Select **Configure** from the navigation panel.
2. Select the **Security** tab and the **Switch Binding** tab. The **Switch Binding** tab view displays (Figure 16).
3. Add the node to the list in one of the following ways:
   - Select an attached node from the **Attached Nodes** drop down list.
   - Type the WWN of a detached node in the **Detached Node** *(WWN)* field.
4. Select the **Add Member** button next to the node that you wish to add. The tab view refreshes and the node is now listed in the SBML at the bottom of the screen.

Deleting a List Member

WWNs can only be removed from the SBML if any of the following are true:

- The director or switch is offline.
- Switch Binding is disabled.
- The switch or device with the WWN is not currently connected to the director or switch (detached node).
- Switch Binding is not enabled for the same port type as enabled for the connection policy. For example, a WWN for a switch attached to an E_Port can be removed if the Switch Binding connection policy is set to **Enabled & Restrict F_Ports**.
- The switch or device with the WWN is connected to a port that is blocked.

To delete a member from the SBML, perform the following procedure:

1. Select **Configure** from the navigation panel.
2. Select the **Security** tab and the **Switch Binding** tab. The **Switch Binding** tab view displays (Figure 16).
3. Select the **Delete** button next to the listing for the member.
4. At the `Are you sure you want to delete this member?` prompt, click **OK**. The SBML redisplays without the deleted member.

Configuring Fabric Binding

Fabric Binding functionality, provided by the SANtegrity Binding feature, allows you to bind the switch or director to specified fabrics so that it can communicate only with those fabrics. With Fabric Binding enabled, the product can communicate only with fabrics that are included in the Fabric Binding Membership List (FBML).

Using Fabric Binding, you can allow specific switches to attach to specific fabrics in the SAN. This provides security from accidental fabric merges and potential fabric disruption when fabrics become segmented because they cannot merge.

The **Fabric Binding** tab allows the user to modify Fabric Binding configuration, to save and activate any changes that have been made to Fabric Binding configuration, and to deactivate Fabric Binding. Fabric Binding is available only if the SANtegrity Binding feature is installed.

Fabric Binding Membership Terminology

The following terms apply to FBMLs and their members, as they are configured using the EWS interface. Two types of FBMLs are configured using the **Fabric Binding** tab.

- Active FBML — When fabric binding is active, the active FBML is the list of fabric members with which the product is allowed to communicate. If fabric binding is disabled, this list is empty.
- Pending FBML — A list shown on the **Fabric Binding** tab, used to configure an FBML before it is made active on the product. Changes to the pending FBML are not implemented in the fabric until they are saved and activated.

The following terms apply to the switches or directors that are part of the FBMLs:

- Local — The switch or director product that you are configuring. This is a required FBML member.
- Attached — A switch or director that is currently in a fabric with the local product. Any switch or director that is attached is a required FBML member.
- Unattached — A switch or director that is not currently in a fabric with the local product. These switches and directors are unattached if they have been added manually to the pending FBML, or if the ISL between the local product and the switch or director was removed.

Enable, Disable, and Online State Functions

In order for Fabric Binding to function, specific operating parameters and optional features must be enabled. Also, there are specific requirements for disabling these parameters and features when the director or switch is offline or online. Be aware of the following:

- Because switches are bound to a fabric by WWN and domain ID, the Insistent Domain ID function is automatically enabled if Fabric Binding is enabled. You cannot disable Insistent Domain ID while Fabric Binding is active and the switch is online. (For information about configuring the domain ID of the product, see “Configuring Operating Parameters” on page 38.)
- If Fabric Binding is enabled and the switch is online, you cannot disable Insistent Domain ID.
- If Fabric Binding is enabled and the director or switch is offline, you can disable Insistent Domain ID, but this will disable Fabric Binding.
- You cannot disable Fabric Binding if Enterprise Fabric Mode is enabled. However, if Enterprise Fabric Mode is disabled, Fabric Binding can be enabled or disabled.

Parts of the Fabric Binding Tab

Open the **Fabric Binding** tab by selecting **Configure** from the navigation panel. Next, select the **Security** tab and the **Fabric Binding** tab. The **Fabric Binding** tab view displays (Figure 17).

Figure 17: Configuring Fabric Binding

The Fabric Binding tab is divided into sections by the following headings:

- Fabric Binding Status—Identifies whether Fabric Binding is active or inactive on the product.
- Actions to Modify the Active Fabric Binding Membership List (FBML)—Enables you to activate and deactivate Fabric Binding using the following buttons:
  - — Activate — By selecting this button, you save the pending FBML as the active FBML and activate Fabric Binding.
  - — Deactivate — By selecting this button, you change the Fabric Binding status from active to inactive, disabling Fabric Binding.

- Actions to Modify the Pending Fabric Binding Membership List (FBML)—Enables you to modify the pending FBML using the following buttons:
  - Delete All — By selecting this button, you can delete all members from the pending FBML that are not attached to the current fabric. Members that are attached must remain in the list, because the membership list must contain all attached members to be activated.
  - Load Active — By selecting this button, you can copy the contents of the active FBML to the pending FBML. The added members may include unattached members of the active FBML.
  - Update — By selecting this button, you can update the pending FBML to include all currently attached fabric members. Unattached members of the active FBML are not added to the list by this action.
  - Add — By selecting this button, you can add a new member to the FBML as defined in the **Domain ID** and **WWN** fields below the button.
- The Pending Fabric Binding Membership List—Enables you to view the pending FBML as it is being updated and to delete unattached members from the list. Members of the pending FBML are listed by WWN. For more information, see "Viewing the Pending FBML" on page 70.

Checking Fabric Binding Status

To determine the status of Fabric Binding on the product, perform the following procedure:

1. Select **Configure** from the navigation panel.
2. Select the **Security** tab and the **Fabric Binding** tab. The **Fabric Binding** tab view displays (Figure 17).
3. The **Fabric Binding Status** parameter shows whether Fabric Binding is active or inactive on the product.

Activating Fabric Binding

When you enable Fabric Binding from the **Fabric Binding** tab, the pending FBML is saved and becomes the active FBML. Before activating Fabric Binding, you may want to configure the Pending FBML. For more information, see "Configuring the Pending FBML" on page 67.

Note: Fabric Binding is also enabled automatically, when the Enterprise Fabric Mode is enabled. However, in this case, only attached fabric members are included in the active FBML. For more information, see "Fabric Binding and the Enterprise Fabric Mode" on page 72.

1. Select **Configure** from the navigation panel.
2. Select the **Security** tab and the **Fabric Binding** tab. The **Fabric Binding** tab view displays (Figure 17).
3. To activate Fabric Binding, select the **Save and Activate** button. All members of the pending FBML are activated on the switch.

Deactivating Fabric Binding

Note: You cannot deactivate Fabric Binding if Enterprise Fabric Mode is enabled.

To deactivate Fabric Binding, perform the following procedure:

1. Select **Configure** from the navigation panel.
2. Select the **Security** tab and the **Fabric Binding** tab. The **Fabric Binding** tab view displays (Figure 17).
3. Select the **Deactivate** button. The Fabric Binding status changes from active to inactive.

Configuring the Pending FBML

You can use any of multiple methods to populate and configure the pending FBML. Consider the following methods:

- To see whether the pending FBML is identical to the active FBML list, see "Determining If the Pending FBML and Active FBML Are Identical" on page 68.
- To manually add list members, see "Adding to the Pending FBML" on page 68.
- To manually delete list members, see "Deleting a Member from the Pending FBML" on page 69.

- To populate the pending FBML with the active FBML list, see "Loading All Active FBML Members to the Pending FBML" on page 69.
- To populate the pending FBML with all of the attached switches or directors, see "Loading Only Attached Members to the Pending FBML" on page 70.

Determining If the Pending FBML and Active FBML Are Identical

The **Fabric Binding** tab indicates whether the pending FBML and the active FBML are identical.

1. Select **Configure** from the navigation panel.
2. Select the **Security** tab and the **Fabric Binding** tab. The **Fabric Binding** tab view displays (Figure 17).
3. Under the **Actions to Modify the Pending Fabric Binding Membership List (FBML)** heading is text that indicates whether the pending FBML is *identical to* or *different from* the active FBML.

If you want the pending FBML to match the active FBML, follow the procedure in "Loading All Active FBML Members to the Pending FBML" on page 69.

Adding to the Pending FBML

Add members to the pending FBML using their WWN and domain ID. The combination of WWN and domain ID cannot be a duplicate of another participant in the fabric. The pending FBML can contain a maximum of maximum of 239 members. To add a new member to the pending FBML, perform the following procedure:

1. Select **Configure** from the navigation panel.
2. Select the **Security** tab and the **Fabric Binding** tab. The **Fabric Binding** tab view displays (Figure 17).
3. At the bottom of the **Actions to Modify the Pending Fabric Binding Membership List (FBML)** section, add a domain ID for the fabric member in the **Domain ID** field. The value of the domain ID is a number in the range 1 to 239.
4. In the **WWN** field, type the WWN of the switch or director.
5. Select the **Add** button. The pending FBML redisplays, showing the added fabric member.

Note: The added members of the pending FBML do not participate in Fabric Binding until the list is saved and activated. To activate the pending FBML, see "Activating the Pending FBML" on page 70.

Deleting a Member from the Pending FBML

To delete a member of the pending FBML, perform the following procedure:

1. Select **Configure** from the navigation panel.
2. Select the **Security** tab and the **Fabric Binding** tab. The **Fabric Binding** tab view displays (Figure 17).
3. Under the heading **Pending Fabric Binding Membership List**, you will find each list member ordered by domain ID and WWN. Click the **Delete** button next to the entry that you want removed from the list.

Note: You cannot delete entries on the pending FBML that are local or attached. Only unattached list members can be deleted.

4. A dialog box displays with the message `Are you sure you want to delete this member?` Click **OK** to delete the member. The pending FBML redisplays, without the deleted entry.

Loading All Active FBML Members to the Pending FBML

As a starting point for populating the pending FBML for editing, you may want to start with a list that contains all of the entries in the active FBML. The active FBML contains the local and attached fabric members and any unattached fabric members that may exist.

To load the active FBML to the pending FBML, perform the following procedure:

1. Select **Configure** from the navigation panel.
2. Select the **Security** tab and the **Fabric Binding** tab. The **Fabric Binding** tab view displays (Figure 17).
3. Under the heading **Pending Fabric Binding Membership List**, select the **Load Active** button. The entire contents of the active FBML are copied to the pending FBML.

Loading Only Attached Members to the Pending FBML

As an efficient starting point for populating the pending FBML for editing, you may want to start with a list that contains the entries that are required for the pending FBML to become active. These entries are the attached fabric members. (In this case, the local fabric member is also added to the pending FBML.)

To load all attached members to the pending FBML, perform the following procedure:

1. Select **Configure** from the navigation panel.
2. Select the **Security** tab and the **Fabric Binding** tab. The **Fabric Binding** tab view displays (Figure 17).
3. Under the heading **Pending Fabric Binding Membership List**, select the **Update** button. All switches and directors in the fabric are copied to the pending FBML.

Activating the Pending FBML

The procedure for activating the pending FBML is the same as for activating Fabric Binding. For instructions, see "Activating Fabric Binding" on page 66.

Viewing the Pending FBML

The **Fabric Binding** tab enables you to view the pending FBML as it is being updated. Members of the pending FBML are listed by WWN. To view the pending FBML list, use the following procedure:

1. Select **Configure** from the navigation panel.
2. Select the **Security** tab and the **Fabric Binding** tab. The **Fabric Binding** tab view displays (Figure 17).
3. Find the pending FBML at the bottom of the page under the heading **Pending Fabric Binding Membership List**.

The pending FBML can contain a maximum of 239 members. The page can show up to 64 members. If the list contains more than 64 members, the other members are shown on subsequent pages. To see the next page of list members, select the **Next >>** link. To see the previous page of members, select the **<< Prev** link. A status line at the top and bottom of the list shows which members are currently displayed and the total number of members in the list.

Configuring Enterprise Fabric Mode

Select **Configure** from the navigation panel. Select the **Security** tab and the **EFM** tab; the **Enterprise Fabric Mode** tab view displays (Figure 18). The Enterprise Fabric Mode automatically enables the features that FICON devices need to participate in a fabric. These features are described in "Features and Parameters Enabled with Enterprise Fabric Mode" on page 71.

Using this view, you can enable or disable the Enterprise Fabric Mode on the product. If the page displays `Enterprise Fabric Mode is Disabled`, selecting **Enable** will enable the mode. If the page displays `Enterprise Fabric Mode is Enabled`, selecting **Disable** will disable the mode.

Although Enterprise Fabric Mode is not a keyed feature, its function depends on Fabric Binding and Switch Binding features that are enabled by the SANtegrity Binding licensed feature. To enable Enterprise Fabric Mode, the SANtegrity Binding feature has to be installed on all the switches and directors in the fabric.

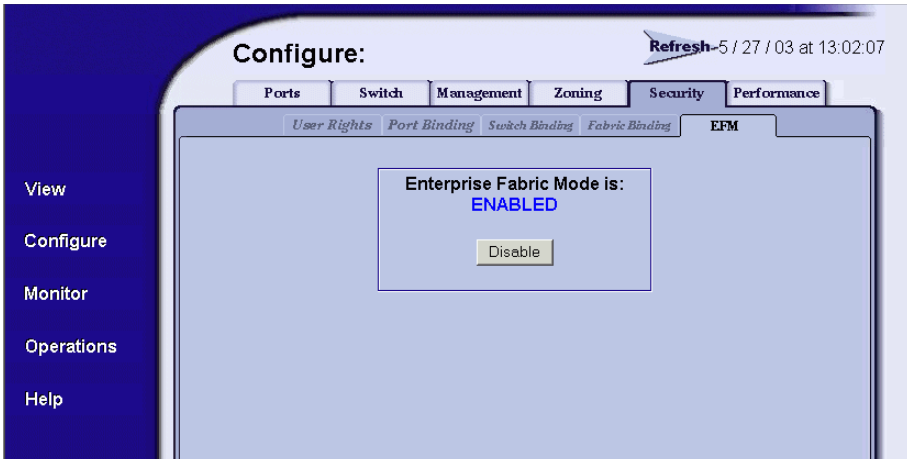


Figure 18: Enabling Enterprise Fabric Mode

Features and Parameters Enabled with Enterprise Fabric Mode

The features that are automatically enabled when Enterprise Fabric Mode is enabled are described in the following sections:

- "Fabric Binding and the Enterprise Fabric Mode" on page 72
- "Switch Binding and the Enterprise Fabric Mode" on page 72
- "Rerouting Delay and the Enterprise Fabric Mode" on page 72

Fabric Binding and the Enterprise Fabric Mode

Fabric Binding is a SANtegrity Binding feature that prohibits switches and directors from communicating with switches or directors that are not part of the fabric. Refer to "Configuring Fabric Binding" on page 63 for details on configuring Fabric Binding.

When the Enterprise Fabric Mode is enabled, Fabric Binding is enabled automatically. The fabric members that are currently attached to the product are added automatically to the active Fabric Binding Membership List (active FBML), a list of switches and directors that are allowed to communicate with the product. Therefore, when Enterprise Fabric Mode is enabled, the fabric members that are currently attached to the product participate in Fabric Binding. To add other fabrics to the active FBML, see "Configuring the Pending FBML" on page 67.

Switch Binding and the Enterprise Fabric Mode

Switch Binding is a SANtegrity Binding feature that enables switches or directors to communicate only with devices that are listed on the Switch Binding Membership List (SBML). When the Enterprise Fabric Mode is enabled, Switch Binding is also enabled. You need to configure the SBML, which specifies the devices with which the switch or director can communicate. Refer to "Configuring Fabric Binding" on page 63 for details on configuring Switch Binding.

Rerouting Delay and the Enterprise Fabric Mode

Rerouting Delay ensures that frames are delivered through the fabric to their destination in the correct order, even if the path changes. If traffic to a particular destination is going to be rerouted over a shorter path, the rerouting delay function prevents new traffic from being released before the existing traffic arrives at its destination.

If a change to the fabric topology creates a new path (for example, a new switch is added to the fabric), frames may be routed over this new path if its hop count is less than a previous path with a minimum hop count. This situation could result in frames being delivered to a destination out of order because frames sent over a new, shorter path may arrive before frames sent previously using the older, longer path.

If Rerouting Delay is enabled, traffic ceases in the fabric for the time specified in the **E_D_TOV** field of the **Configure Fabric Parameters** dialog box (for more information, see "Configuring Fabric Parameters" on page 41). This delay enables frames sent using the old path to arrive at their destination before frames begin traversing the new path.

If Enterprise Fabric Mode is enabled, Rerouting Delay is automatically enabled and cannot be disabled unless the director or switch is offline. In this case, disabling Rerouting Delay also disables Enterprise Fabric Mode. For information about configuring and enabling Rerouting Delay, see "Configuring Operating Parameters" on page 38.

Domain RSCNs and the Enterprise Fabric Mode

Domain register for state change notifications (domain RSCNs) are sent between end devices in a fabric to provide additional connection information to host bus adapters (HBA) and storage devices. As an example, this information might be that a logical path has been broken because of a physical event, such as a fiber optic cable being disconnected from a port.

If Enterprise Fabric Mode is enabled, Domain RSCNs are automatically enabled and cannot be disabled unless the director or switch is offline. In this case, disabling Domain RSCNs also disables Enterprise Fabric Mode. For information about enabling Domain RSCNs, see "Configuring Operating Parameters" on page 38.

Insistent Domain Identification (ID) and the Enterprise Fabric Mode

If enabled, Insistent Domain ID specifies that the preferred domain ID configured for the product will be the product's active domain identification when the fabric initializes. For information about configuring the preferred domain ID, see "Configuring Operating Parameters" on page 38.

A static and unique domain ID is required by the Fabric Binding feature because the feature's FBML identifies switches by WWN and domain ID. If a duplicate preferred domain ID is used, then made insistent, warnings display when directors and switches are added to an FBML.

If Fabric Binding or Enterprise Fabric Mode is enabled, Insistent Domain ID is automatically enabled and cannot be disabled unless the director or switch is offline. In this case, disabling Insistent Domain ID disables Enterprise Fabric Mode and Fabric Binding. For information about configuring the domain ID and Insistent Domain ID, see "Configuring Operating Parameters" on page 38.

Configuring Open Trunking

The **Open Trunking** page enables you to configure open trunking settings. Open Trunking is an optional software feature that is enabled using a feature key.

The purpose of Open Trunking is to make efficient use of redundant interswitch links (ISLs) between neighboring switches by means of load balancing. ISLs are fiber optic cables that connect ports between Fibre Channel switches and link these switches into a multiswitch fabric. Fibre Channel traffic flows through these ISLs from end devices (servers and storage devices) attached to ports on individual switches.

When the traffic on a particular port exceeds a specified threshold, the Open Trunking functionality routes some of the traffic to another ISL. This prevents traffic from becoming congested on an ISL. Open trunking provides automatic, dynamic, statistical traffic load balancing across ISLs in a fabric environment.

The Open Trunking feature monitors Fibre Channel data rates through multiple ISLs, dynamically applies a fibre shortest path first (FSPF) networking algorithm to calculate the optimum path between fabric elements, and balances the Fibre Channel traffic load accordingly. The objective is to make the most efficient possible use of redundant ISLs between neighboring switches, even if these ISLs have different bandwidths.

The Open Trunking feature monitors the average data rates of all traffic flows (from a transmit port to a destination domain), and periodically adjusts routing tables to reroute data flows from congested links to lightly loaded links and optimizes bandwidth use.

Load-balancing among the ISLs does not require user configuration, other than enabling open trunking and selecting optional or default settings for congestion thresholds (per port) and a response threshold for lack of BB_Credits. In particular, you do not need to manually configure ISLs into trunk groups of redundant links where data can be off-loaded.

Candidate links for rerouting flow are identified automatically and maintained by the FSPF protocol. All ISLs that lead to adjacent switches on the shortest path to the flow's destination are considered. This means that even if a link is not on the shortest path to the destination, the flow may be rerouted to this link to relieve congestion. This also means that flow may be rerouted onto a link that goes to a different adjacent switch.

Note: For the Director 2/140, ports are displayed through several pages in groups of 32. To configure all of the ports, make sure you go through each set. You must click **Activate** for each view before moving to the next.

To configure Open Trunking:

1. Choose **Configure** from the navigation panel.
2. Choose the **Performance** tab and the **Open Trunking** tab. The **Open Trunking** tab view displays (Figure 19).

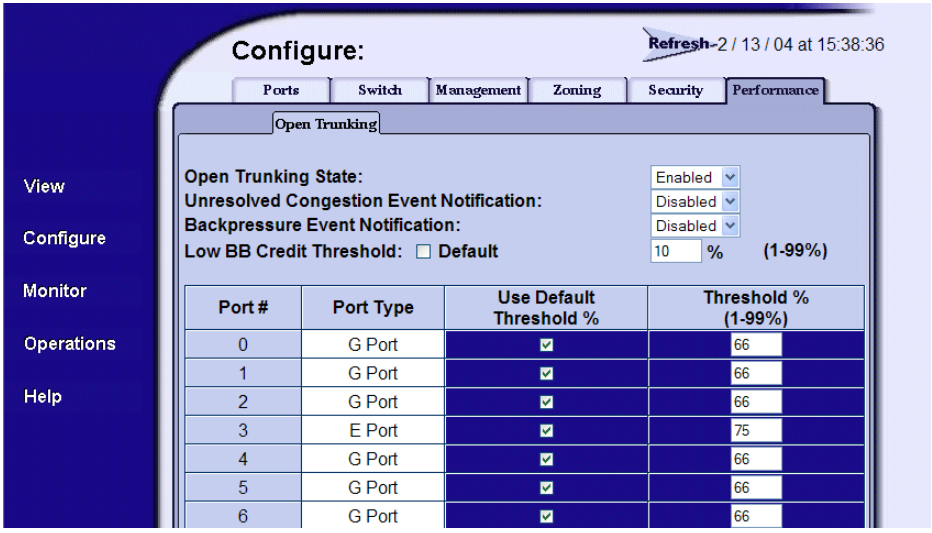


Figure 19: Configuring Open Trunking

3. Choose **Enabled** in the **Open Trunking State** drop down list.
4. Choose **Enabled** or **Disabled** from the **Unresolved Congestion Event Notification** drop down list. If enabled, an unresolved congestion entry is made in the event log and, if SNMP is configured, an SNMP trap is generated. Unresolved congestion occurs when a flow cannot be rerouted to another link because it would exceed the other link's threshold.
5. Choose **Enabled** or **Disabled** from the **Backpressure Event Notification** drop down list. If enabled, a backpressure entry is made in the event log and, if SNMP is configured, an SNMP trap is generated. Backpressure occurs when the threshold of unavailable BB_Credits is exceeded for any link.
6. Specify a value for the **Low BB Credit Threshold** option, if desired.

Note: Earlier versions of this dialog box may display **Credit Starvation Threshold** instead of the **Low BB Credit Threshold**.

The system monitors the percentage of time that the port experiences no transmit BB_credits on the link. The link cannot transmit without BB_credits. When the threshold is exceeded, the system reroutes flows away from the ISL that is experiencing this problem. This threshold is also used to prevent rerouting of traffic to an ISL that is experiencing a low BB_credit threshold condition. The enabled **Default** check box indicates that the default threshold value of 10% should be used rather than the value in the **%** entry field. This parameter must be a value in the range 1 to 99, if the **Default** box is not checked.

7. Specify a load-balancing threshold value in the **Threshold %** field for each port, if desired. Use this field to configure the value of the load-balancing threshold for each port. When this threshold is exceeded, the open trunking functionality offloads some of the traffic to another ISL. The threshold must be a value in the range 1 to 99, if the **Default** box is not checked.
8. Click the **Activate** button at the bottom of the screen.

Installing Feature Keys

Perform this procedure to install one or more of the following optional features:

- **OSMS** — The Open Systems Management Server feature allows open systems host control of the product.
- **FICON Management Server** — The FICON Management Server feature allows host control and inband management of the director or switch through an IBM System/390 or zSeries 900 Parallel Enterprise Server server attached to a director or switch port. The server communicates with the switch or director through a FICON channel.
- **Flexport** — A Flexport switch is delivered at a discount with only a portion of the switch's ports enabled. When additional port capacity is required, the remaining ports are enabled through purchase of this feature. Ports are enabled in increments of eight except for the Edge Switch 2/12, for which ports are enabled in groups of four.
- **Fabric Capable** — An Edge Switch 2/12 cannot participate in a fabric unless this feature is purchased. When this feature is installed, ports on the Edge Switch 2/12 can be defined as E_Ports, G_Ports, or GX_ports. (Installation of this feature also changed the BB_Credit settings on ports from 5 to 12.)
- **SANtegrity Binding** — This feature enhances security in SANs, which is valuable in SANs that contain a large or heterogeneous group of fabrics and attached devices.
- **Open Trunking** — This feature enhances efficiency in the use of redundant ISLs between neighboring switches by means of load balancing. This prevents traffic from becoming congested on an ISL.

After purchasing a feature, obtain the required feature key from the web site to which the feature documentation directs you. A feature key is an alphanumeric string consisting of both uppercase and lowercase characters. The total number of characters may vary depending on keys and serial number. The feature key is case-sensitive and must be entered exactly, including dashes.

Feature keys use a format similar to the following:

XxXx-XXxX-xxXX-xX.

Note: You must be logged in with Administrator-level rights to install feature keys.

The feature key can be installed while the product is online, except in the following circumstances:

- With E/OS 3.0 or earlier, the product must be offline before a feature can be enabled.
- If the new feature key removes existing functionality, the product must be offline during the installation process.

(See "Setting Product Online or Offline" on page 137 for instructions on setting the product offline.)

After obtaining the feature key, install the feature as follows:

1. Choose **Operations** from the navigation panel. The **Operations** page opens.
2. Click the **Feature Installation** tab. The **Feature Installation** tab view displays (Figure 20).

Note: If the new feature key is removing an existing feature of your system, you must set the switch offline before completing the feature activation process.

Figure 20: Feature Installation tab view

3. Type the feature key and click **Activate**. The interface displays a confirmation page with a warning, stating this action overrides the current set of product features.

Note: When **Activate** is selected, all current features are removed and replaced with the features specified in the feature key. Features not included in the new feature key are no longer available on the system. Because of this, it is important to verify that the feature key enables all desired features.

4. Click **Activate** to activate the new feature key. (The system automatically undergoes an IPL).

Note: If you receive the error message, `Error 238, Invalid Key`, it means that either the feature key was entered incorrectly or the feature key is not a valid key for that feature. Re-enter the feature key. If you continue to have problems, contact technical support.

Saving Configuration Information

After changing your system configuration, you may want to save a current listing of configuration information. Although EWS does not allow for a system restoration, you can use this information to restore system settings. This information also may be requested by technical support to help resolve technical problems.

To save configuration information, view the product information page as described in "Obtaining Product Information" on page 148. Use your browser to Save the product information page to a file. (You may also want to print the output for quick reference.)

Configuring Zones

3

This chapter provides an overview of zoning and describes how to configure zones and zone sets. This chapter includes the following topics:

Understanding Zoning

Designing zoning can be a complex task, especially for multiswitch fabrics. Consult with your managed product vendor's professional services organization before configuring zoning.

This section is designed to help you understand the following concepts so that you can more efficiently use Embedded Web Server features to configure and manage zones across a multiswitch fabric:

- Benefits of zoning.
- How zoning works to control access to storage devices and servers across a fabric.
- Other methods of controlling access at the switch and at the server and device, such as binding.
- Merging zoned fabrics.
- Basic terms and concepts of zoning that you must understand when configuring zoning.

Controlling Access Across a Fabric

Embedded Web Server zoning features enable you to establish zoning across a fabric of devices attached to switches and directors by partitioning these devices into groups called zones. A zone consists of devices that can access each other through port-to-port connections. Devices in the same zone can recognize and communicate with each other; devices in different zones cannot.

System administrators create zones to increase security and prevent data loss or corruption by controlling access between devices (such as servers and data storage units), or between separate user groups (such as engineering or human resources).

Zoning allows an administrator to:

- Establish barriers between devices that use different operating systems. For example, it is often critical to separate servers and storage devices with different operating systems because accidental transfer of information from one to another can delete or corrupt data. Zoning prevents this by grouping devices that use the same operating systems into zones.
- Create logical subsets of closed user groups. Administrators can authorize access rights to specific zones for specific user groups, thereby protecting confidential data from unauthorized access.

- Create groups of devices that are separate from devices in the rest of a fabric. Zoning allows certain processes (such as maintenance or testing) to be performed on devices in one group without interrupting devices in other groups.
- Allow temporary access between devices for specific purposes. Administrators can remove zoning restrictions temporarily (for example, to perform nightly data backup), then restore zoning restrictions to perform normal processes.

Figure 21 illustrates three zones established on a single managed product with four devices in each zone. Devices in each zone can communicate with and access devices only in their respective zones.

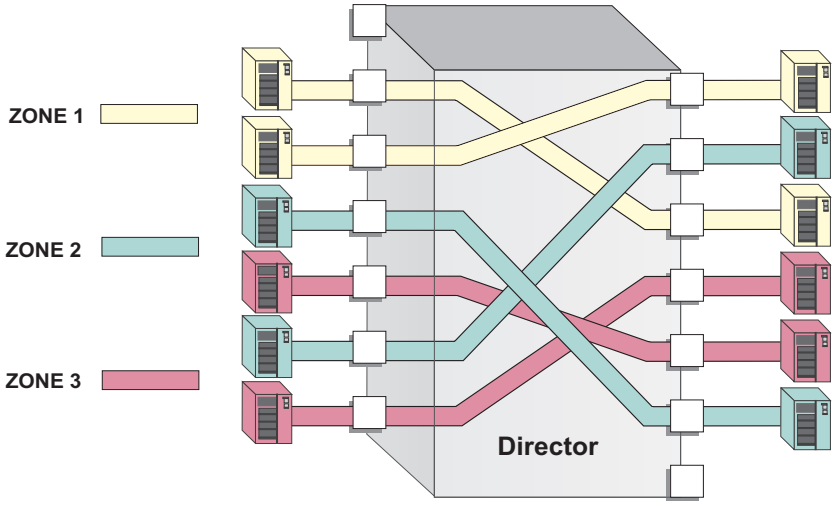


Figure 21: Zoning through a single Fibre Channel managed product

Figure 22 illustrates how zones can consist of ports and/or devices installed on ports in three managed products in a multiswitch fabric.

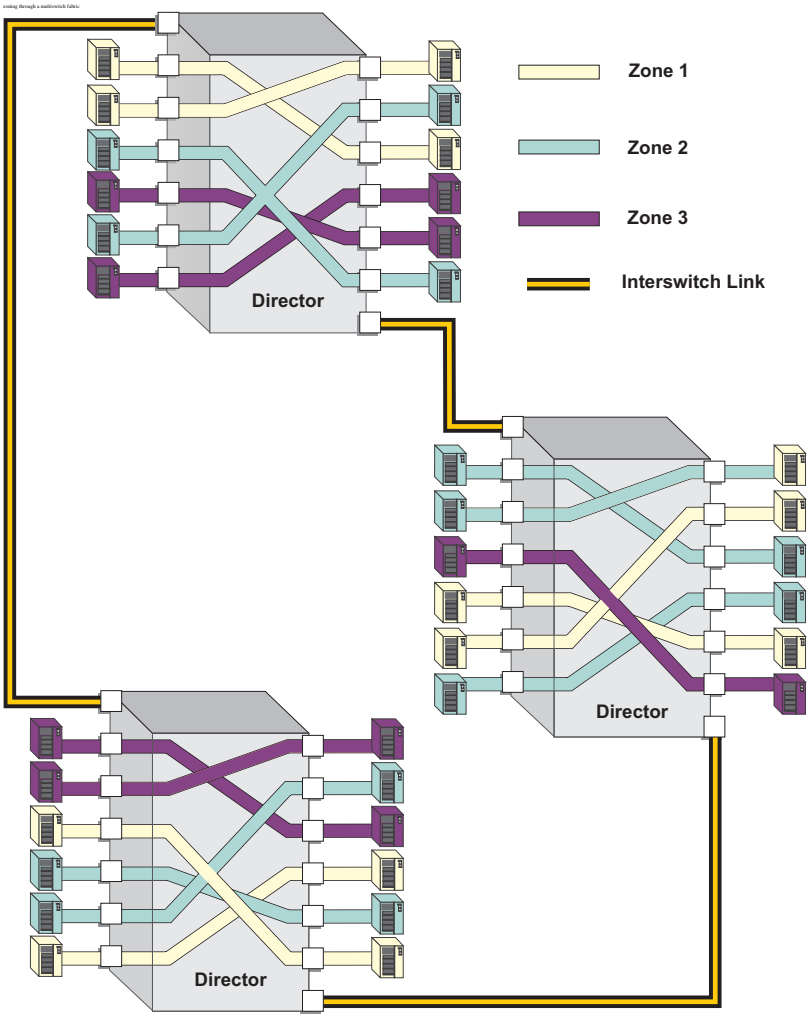


Figure 22: Zoning through a multiswitch fabric

Controlling Access at the Switch

A port binding feature is available on switches and directors that allows you to *bind* a specific switch or director port to the WWN of an attached device for exclusive communication. This Port Binding feature is available through the **Port Binding** tab, which is under the **Security** tab of the **Configure** page view.

Controlling Access at the Server or Storage Device

Features available at the server or storage device can add methods, beyond zoning, to increase network security measures, differentiate between operating systems, and prevent data loss or corruption by controlling access between devices or between separate user groups (such as engineering or human resources).

Server-level access control is called persistent binding. Persistent binding uses configuration information stored on the server and is implemented through the server's host bus adapter (HBA) driver. The process binds a server device name to a specific Fibre Channel storage volume or logical unit number (LUN), through a specific HBA and storage port WWN. In essence, this feature creates a reliable route across the fabric that sustains the small computer system interface (SCSI) connection between a server and storage device.

For persistent binding:

- Each server HBA is explicitly bound to a storage volume or LUN, and access is explicitly authorized (access is blocked by default).
- The process is compatible with open system interconnection (OSI) standards. The following are transparently supported:
  - Different operating systems and applications.
  - Different storage volume managers and file systems.
  - Different fabric devices, including disk drives, tape drives, and tape libraries.
- If the server is rebooted, the server-to-storage connection is automatically re-established.
- The connection is bound to a storage port WWN. If the fiber-optic cable is disconnected from the storage port, the server-to-storage connection is automatically re-established when the port cable is reconnected. The connection is also automatically re-established if the storage port is cabled through a different managed product port.

Access can also be controlled at the storage device as an addition or enhancement to redundant array of independent disks (RAID) controller software. Data access is controlled within the storage device, and server HBA access to each LUN is explicitly limited (access is blocked by default). Storage-level access control:

- Provides control at the storage port and LUN level, and does not require configuration at the server.

- Is typically proprietary and protects only a specific vendor's storage devices. Storage-level access control may not be available for many legacy devices.

Before establishing persistent binding or access control features at the storage device, consult with your managed-product vendor's professional services organization.

Zoning Concepts

Zoning is configured by authorizing or restricting access to name server information associated with device ports that attach to product ports. A zone member is specified by the number of the product port to which a device is attached, or by the 8-byte WWN assigned to the HBA or Fibre Channel interface installed in a device. A device port can belong to multiple zones.

Zoning concepts include:

- Zones
- Default Zone
- Zone Sets
- Active Zone Set

Naming Conventions for Zones and Zone Sets

The following naming conventions apply to zones and zone sets:

- All names must be unique and may not differ by case only. For example, myzone and MyZone are both valid individually, but they are not unique.
- The first character of a zone set name must be a letter (A—Z, a—z).
- A zone set name cannot contain spaces.
- Valid characters are a—z, A—Z, 0—9, ^, -, _, and $.
- A zone set name can have a maximum of 64 characters.

Zones

A zone contains a set of members that can access each other. Refer to Table 3 for details on the number of members that you can configure in a zone and the number of zones that you can configure with the EWS Configure Zone functions.

A zone member can be a switch or director port or the WWN of the device. Ports and devices spread throughout multiple managed products in a multiswitch fabric may be grouped into the same zone. Members of a zone can see each other; members in different zones cannot. The number of members that you can

configure for a zone varies according to the number of zones in the zone set, the length of the zone names, and other factors, but is essentially bounded by the available nonvolatile random-access memory (NVRAM) in the managed product.

Note: Port numbers cannot be used for zone members if the interoperability mode for the switch or director is set to Open Fabric 1.0 mode. In this case, you must use node WWNs as zone members.

The type of zone members identified for a zone may be mixed and matched. For example, two members may be specified by a port number and the third member by the WWN of the device.

Using WWNs

To identify a zone member by WWN, use the 16-digit WWN of the device. For example:

10:00:08:00:88:40:C0:D4

In EWS the WWN displays with the switch or director manufacturer's name before the WWN. The WWN is assigned to the Fibre Channel interface or HBA installed in devices such as servers or storage devices. Although the device may also have a node WWN, this WWN is not used for zoning identification.

Note: Nicknames can be assigned to the WWN using the HAFM Product Manager. This functionality is not available in EWS.

The advantage of identifying a zone member as the WWN of the attached device is that the identification will not change if fiber cable connections to ports are rearranged. This is especially important if you are using spare ports. You can simply move the fiber cable to a spare port from a failed port and still maintain the zoning configuration.

The disadvantage of identifying a zone member by the WWN is that removal and replacement of a device HBA or Fibre Channel interface (thereby changing the device WWN) disrupts zone operation and may incorrectly include or exclude a device from a zone.

Using Port Numbers

To identify a zone member by port number, use the domain identification number of the managed product and the port number on that managed product. For example:

Domain 1, Port 1

Note: Port numbers cannot be used for zone members if the interoperability mode for the switch or director is set to Open Fabric 1.0 mode.

Port numbers can be 0 through *n*, with *n* representing the number of ports on the managed product minus one. When you define a zone member by a port number, any device attached through that port is included in the zone. A port number that you assign as a zone member is automatically prefixed with the domain identification number of the managed product.

The advantage of identifying a zone member by port number is that if the HBA on an attached device fails, you don't have to identify the member with the WWN of the replacement HBA.

A disadvantage of port zoning is that someone may rearrange cable connections to ports (because of port failures or other reasons) and inadvertently allow devices to communicate that should not have access to each other.

Note: If a managed product's Domain ID changes, you must reconfigure all zones that contained the managed product's port as a zone member. We recommend assigning unique Preferred Domain IDs to each switch in the fabric. You can make these assignments using the EWS **Configure** page**, Switch**, **Parameters** tabs to change the Preferred Domain IDs.

Default Zone

A default zone consists of all devices that have not been configured as members of a zone in a currently-active zone set. The following are some important points to remember about zone sets:

- You can enable or disable the default zone separately from the active zone set by choosing the **Zoning** option from the **Configure** menu. Enabling the default zone allows all devices and ports not configured as members of the active zone set to communicate. If the default zone is disabled, these ports and devices cannot communicate.

- When no zone set is activated, then all devices are considered to be in the default zone.
- If a zone set is active, then all connected devices that are not included as members of a zone in the active zone set are included in the default zone.

Zone Sets

A zone set is a group of zones that you can activate or deactivate as a single entity across all managed products in either a single switch or a multiswitch fabric. Only one zone set can be active at one time. Devices that are members of zones in the zone set can only communicate with members of zones in the same zone set. However, devices can be included as members of more than one zone set. By activating a zone set, you are making all zones in the set active.

The following are some important points to remember about zone sets:

- If no zone set is active, and the default zone is disabled, then no devices can communicate.
- If you activate a zone set when there is already an active zone set, that set will replace the currently-active zone set.
- If you deactivate the current active zone set, then all devices connected in the fabric become members of the default zone.

Active Zone Set

An active zone set is a zone set that is currently active on a single-switch fabric or across all managed products in a multiswitch fabric. At any time, you can disable zoning by deactivating the active zone set and enabling the default zone, or you can enable zoning by activating a zone set. When a zone set is active, all zones that are members of that zone set are active. Only one zone set can be active for the fabric at one time. If no zones are active, then all devices are considered to be in the default zone.

Merging Zoned Fabrics

Managed products are linked through Interswitch Links (ISLs) to form multiswitch fabrics. In a multiswitch fabric, the active zoning configuration applies to the entire fabric. Any change to the configuration applies to all switches in the fabric.

When fabrics join through an ISL, adjacent managed products exchange active zone configurations and determine if the configurations are compatible and can merge. Zoning configurations are compatible if the active zone names in each fabric are unique. If there are identical zone names in each fabric, then the zones must have identical members for the fabrics to join.

If the configurations can merge, the fabrics join. The resulting configuration will be a single zone set containing zone definitions from each fabric.

If configurations cannot merge, the expansion ports (E_Ports) on each product become segmented. Segmented E_Ports cannot carry traffic from attached devices (class 2 or 3 traffic), but can carry management and control traffic (class F traffic) between managed products.

Rules for Merging Zoned Fabrics

Certain rules are enforced to ensure that zoning is consistent across the fabric. Table 3 summarizes rules for joining two fabrics through an ISL. The following terms are used in the table:

- Not zoned — No zone set is active in the fabric and the default zone is enabled. In other words, all devices in the fabric are visible to all other devices in the fabric.
- Zoned — A zone set is active in the fabric and/or the default zone is disabled. In this case, devices can discover other devices that are members of the same zone.
- Zoning configuration — Combination of the active zone set definition and the default zone state (enabled or disabled).

Table 3: Merging Zones

Fabric A	Fabric B	Result
Not zoned	Not zoned	Fabrics join successfully. The new fabric remains not zoned.
Not zoned	Zoned	Fabrics join successfully and the active zone set will propagate across the fabric. Fabric A inherits zoning configuration from Fabric B.
Zoned	Not zoned	Fabrics join successfully and the active zone set will propagate across the fabric. Fabric B inherits zoning configuration from Fabric A.
Zoned	Zoned	Fabrics can merge if the zone names in each fabric are unique. The resulting active zone set is a union of the zones from each fabric. Once you have merged the two zoned fabrics, click the **Save active zone set as** button in the **Zoning view** to save the active zone set. If there is a zone name conflict (the same zone name in each fabric) then the zones must have identical members for the fabrics to join. If the two zones have the same name but contain different members, then the E_Ports will segment and the fabrics will not join.

Note: If merging zones will result in segmented E_Ports and the fabrics will not join, you can join the fabrics by deactivating the active zone set on one of the fabrics (default zone is enabled). This eliminates any conflicts because the fabrics will then join using only the active zone set. After the fabrics join, you can make adjustments to zoning configurations as you desire.

Configuring, Adding, or Deleting Zones

Perform this procedure to configure, change, add, or delete zones. A zone is a group of devices that can access each other through port-to-port connections. Devices in the same zone can recognize and communicate with each other; devices in different zones cannot.

Caution: If, in your business practices, zoning tasks are performed using both the Command Line Interface (CLI) and EWS, you risk potential conflicts in the configuration and functionality could be lost.

To configure zones:

1. Choose **Configure** from the navigation panel.
2. At the **Configure** page, choose the **Zoning** tab and the **Zones** tab. The **Zones** tab view displays as shown in Figure 23.

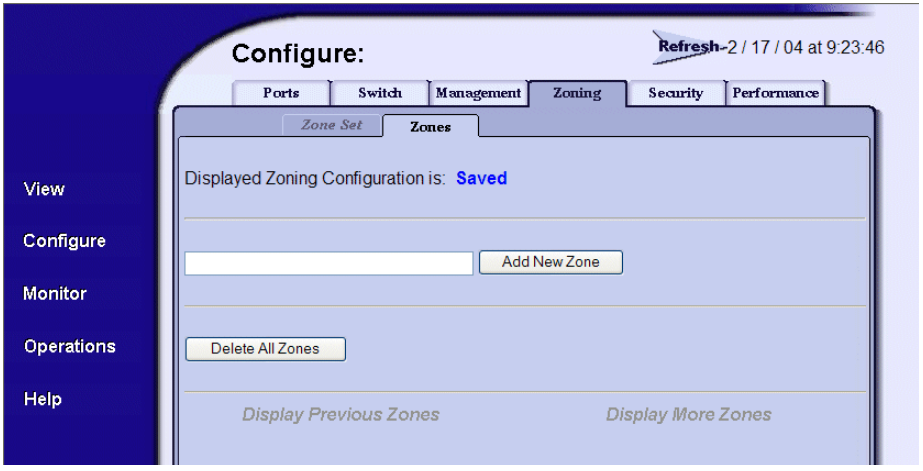


Figure 23: Configuring zones

3. To configure a zone, first add the zone name to the product configuration. The following naming conventions apply to zones and zone sets:
   - All names must be unique and may not differ by case only. For example, **zone-1** and **Zone-1** are both valid individually, but are not considered unique.

- The first character of a zone set name must be a letter (`A` through `Z` or `a` through `z`).
- A zone set name cannot contain spaces.
- Valid characters are alphanumerics and the caret (`^`), hyphen (`-`), underscore (`_`), or dollar (`$`) symbols.
- A zone set name can have a maximum of 64 characters.

Note: A product can have a maximum of 1024 zones.

4. Type the zone name and click **Add New Zone**. After the name is validated, the new zone name (**Zone-1**) and an associated **Delete** button display at the bottom of the page. Note the following:
   - **Save and activate the zone** — Changes to a zone or zoning configuration are not saved and activated on the product until saved as part of a zone set. See "Configuring Zone Sets" on page 96 for information about performing this function.
   - **Delete all zones** — To delete all configured zones and zone members, click **Delete All Zones**. A confirmation dialog box displays. Click **OK** to delete all zones.
   - **Delete a single zone** — To delete a single zone and its zone members, click the **Delete** button adjacent to the zone name. A confirmation dialog box displays. Click **OK** to delete the zone.
   - **Display more zones** — If a zone set contains more than 64 zones, the **Display More Zones** link activates to display subsequent pages. In addition, the **Display Previous Zones** link activates on subsequent displayed pages.
5. To add devices (members) to the zone, click the zone name (**Zone-1**). The **Modify Zone** tab view displays (Figure 24).

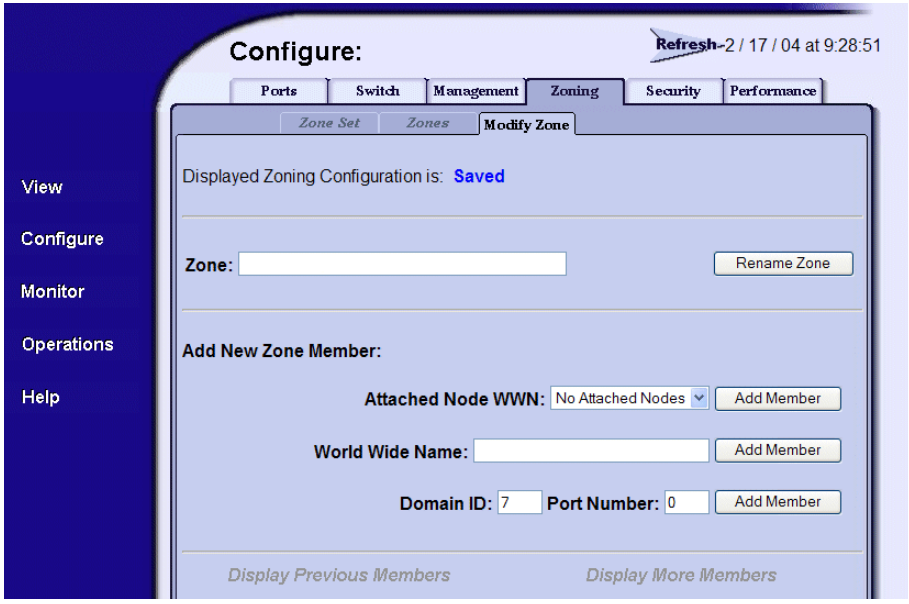


Figure 24: Modify Zone tab view

Rename the zone — To rename a configured zone, type the new name in the **Zone** field and click **Rename Zone**. After the name is validated, the zone name is changed.

6. Nodes may be local to this product or they may be attached to a remote fabric member. Add or delete zone members as follows:

Note: A zone can have a maximum of 1024 zone members. A product can have a maximum of 1024 zone members in its zones.

- **Add member by attached node WWN** — Choose the WWN of an attached device (node) from the **Attached Node World Wide Name** drop-down list and click the **Add Member** button. The device is added to the zone.

Note: The **Attached Node World Wide Name** list is ordered by Domain ID and includes the first 140 attached nodes in the fabric.

- **Add member by WWN** — Type the WWN of a device in the World Wide Name field and click the adjacent Add Member button. The device is added to the zone.
- **Add member by domain ID and port number** — Type the domain ID (1 through 31) of the switch in the **Domain ID** field, type the switch port number to which a device is attached, and click the adjacent **Add Member** button. The device attached to that port is added to the zone.
- **Delete a member** — To delete a zone member, click the **Delete** button adjacent to the configured zone member (WWN or domain ID and port number) at the bottom of the page. A confirmation dialog box displays. Click **OK** to delete the zone member.

7. Changes to a zone, zoning configuration, or zone member are not saved and activated on the switch until saved as part of a zone set. See "Configuring Zone Sets" on page 96 for information about performing this function.
8. Up to 64 zones may be displayed on a single page. If a zone set has more than 64 zones defined, you can display additional pages by choosing **Display Previous Zones** or **Display More Zones**. These fields are grayed out if there are 64 or fewer zones defined for a zone set.

Configuring Zone Sets

Perform this procedure to configure, change, enable, or disable zone sets. A zone set is a group of zones that is activated or deactivated as a single entity across all managed products in either a single switch or a multiswitch fabric. Only one zone set can be active at one time. To configure zone sets:

1. Choose **Configure** from the navigation panel.
2. Choose the **Zoning** tab and the **Zone Set** tab. The **Zone Set** tab view displays (Figure 25).

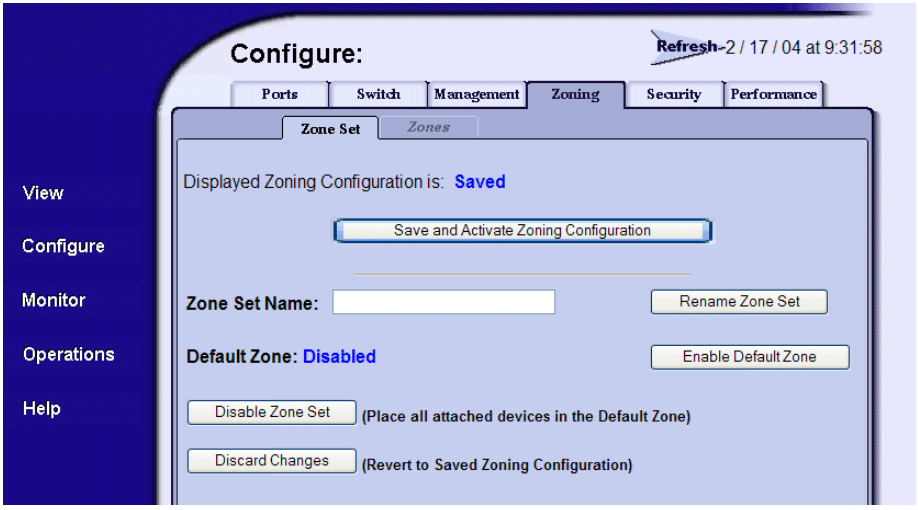


Figure 25: Zone Set tab view

3. Click **Save and Activate Zoning Configuration**. After the zone set name is validated, a confirmation dialog box displays.
4. Click **OK** to save and activate the new zone set. The following message displays: `Your changes to the Zoning configuration have been successfully activated`. Note the following:
   - **Rename zone set** — To rename a zone set, type the new name in the **Zone Set Name** field. Click **Rename Zone Set**. The new zone set name is validated and changed.

Note: If no name is specified, the name NEW_ZONE_SET is used.

- **Enable or disable default zone** — To toggle (enable or disable) the default zone state, click **Enable Default Zone** or **Disable Default Zone**. Depending on the toggle state, the **Default Zone** field changes to **Enabled** or **Disabled**.
- **Disable zone set** — To disable the active zone set and place all attached devices in the default zone, click **Disable Zone Set**. A confirmation dialog box displays. Click **OK** to disable the active zone set.
- **Discard changes** — To discard unsaved changes made to a zone set configuration and revert to a saved zoning configuration, click **Discard Changes**. A confirmation dialog box displays. Click **OK** to discard the changes.

Viewing Product and Fabric Data

4

This chapter describes how to use the Embedded Web Server to view information related to the configuration, status, and communications of a product using the **View** page. You can use EWS to view configuration information for the product and the fabric in which the product participates.

This chapter has been subdivided as follows:

Viewing Product Information

The **View** panel of the EWS interface enables you to see a representation of the physical product, whether a director or switch, and view the various IDs and configuration items for the product.

Viewing a Representation of the Product

To view the representation of the product, choose **View** from the navigation panel. The **View** page opens displaying the **Switch** or **Director** tab view, as appropriate for the product (Figure 26).

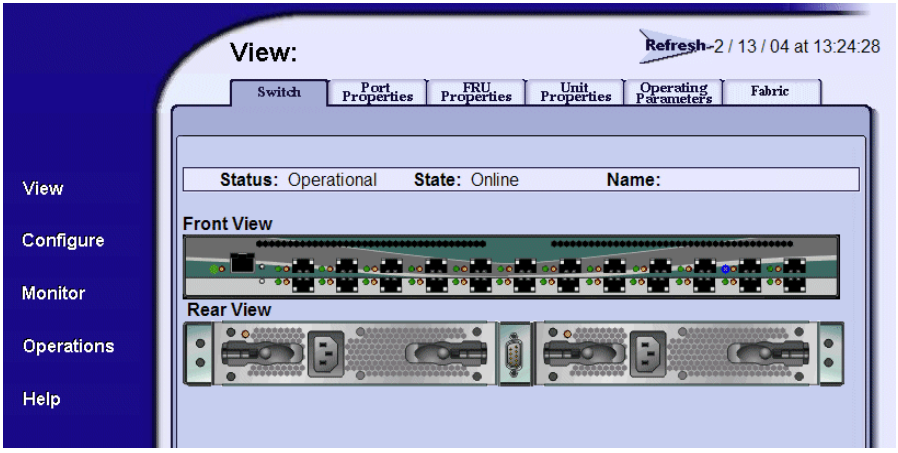


Figure 26: Switch tab view

This page shows the following:

- **Status** — The product's operational status. Possible values are: **Operational**, **Degraded**, and **Failed**.
- **State** — The product's operational state. Possible states are defined in Table 4 on page 101.

Table 4: State Definitions

State	Description
OFFLINE	When the product is OFFLINE, all ports are offline. The ports cannot accept a login from an attached device and cannot connect to other switches. You can configure this state through the **Online State** tab view (See "Setting Product Online or Offline" on page 137 for instructions).
Online	All unblocked ports are able to connect with devices. You can configure this state through the **Set Online State** tab view (See "Setting Product Online or Offline" on page 137 for instructions). Note that the product automatically goes online after a power-up, an initial machine load (IML), or initial program load (IPL).

- **Name** — The user-defined name or description assigned to the product.
- **Front View and Rear View** — Using this graphical view of the product, you can view status symbols and simulated light emitting diode (LED) indicators, display data, or use mouse functions to monitor status and obtain vital product information for the product and its hardware components.

  Move the cursor over parts of the graphics to display labels identifying each hardware component or port and its slot position in the chassis. Choose a port to view the corresponding **Port Properties** tab for the port. Choose an FRU to view the **FRU Properties** tab for the FRU.

  Colored indicators reflect the status of actual LEDs on the product's components. Table 5 describes the port operational states and the LED and attention indicators that display on the **Switch** or **Director** page.

Table 5: Status Indicators

View	LED Name	Color	Behavior
Front	System Power	Green	Off when the LAN is down. On when the LAN is up.
	System Error Light (SEL)	Amber	Off when the SEL on the hardware is off. On when the SEL on the hardware is on. When this indicator illuminates, an event has occurred requiring immediate attention, such as a system, fan, power supply, or port failure.
	Port Online	Green/Blue	Off when port status is anything but Online. Green when port status is Online and the operating speed is 1 Gb/s. Blue when port status is Online and the operating speed is 2 Gb/s (Edge Switch 2/24 only).
	Port Service Required	Amber	Off when port status is anything but Failed or Service Required. On when port status is Failed or Service Required.
Rear	FRU Service Required	Amber	Off when FRU status is Active. On when FRU status is Failed.

Viewing Port Properties

To view the properties of a port on a product, perform the following procedure:

1. Choose **View** from the navigation panel.
2. Choose the **Port Properties** tab. The **Port Properties** tab view displays (Figure 27) showing the properties for only one port.

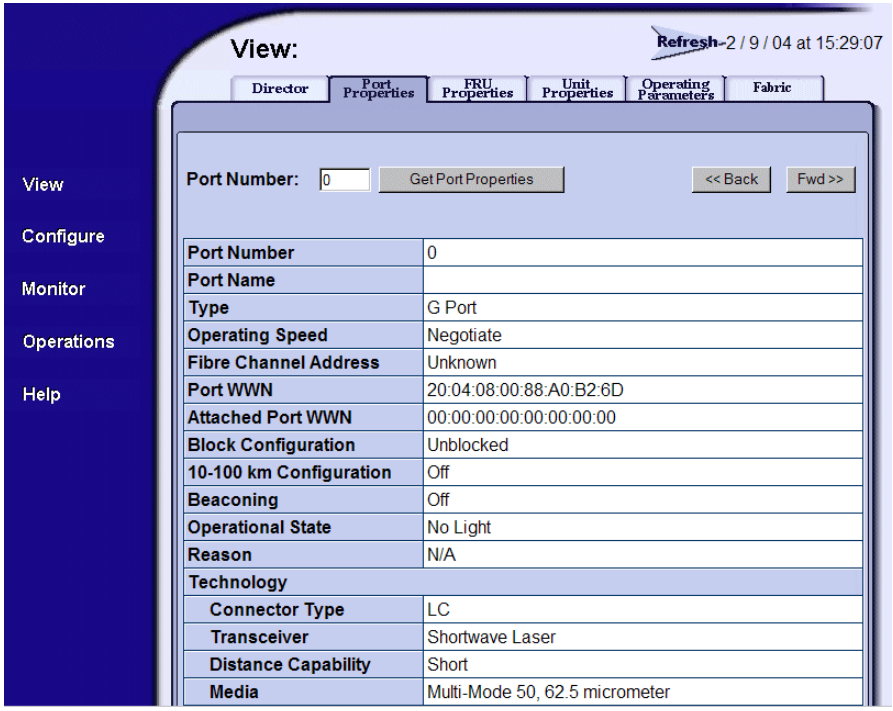


Figure 27: Port Properties tab view

3. To display properties for a specific port, insert the port's number in the **Port Number** field and click the **Get Port Properties** button. (You can also use the **<<Back** and **Fwd>>** buttons to view port information incrementally, one at a time.)

The **Port Properties** page provides the following information:

- **Port Number** — The physical port number.
- **Port Name** — User-defined port name or description.
- **Type**
  - `G_port` — Displays if nothing is logged into the port and the port is configured to be a G_Port.
  - `F_Port` — Displays if a device is logged into the port.
  - `E_Port` — Displays if the port is connected to another switch's E_Port through an ISL.

  - — GX_Port — Valid only on the Edge Switch 2/24; allows a port to operate as either a Fabric Loop Port, Fabric Port, or an Expansion Port. This displays if nothing is logged into the port and the port is configured to be a GX_Port.
  - — FX_Port — Valid only on the Edge Switch 2/24; restricts a port to operate as either a Fabric Loop Port or a Fabric Port.

- **Operating Speed** — This field displays the current data speed for the port as 1 Gb/sec, 2 Gb/sec, or Not Established. Not Established displays if Negotiate is defined as the operating speed and the data speed has not been resolved between the port and the attached device, or if the port and device are not communicating. Note that 2 Gb/sec and Not Established can display only on machines that support 2 Gb/s speeds.
- **Fibre Channel Address** — Fibre Channel Address identifier of the port. Not displayed for some products.
- **Port WWN** — The port's 16-digit WWN.
- **Attached Port WWN** — Fibre Channel WWN identifier of the device attached to the port. (This field is not valid on the Edge Switch 2/24.
- **Block Configuration** — Indicates whether the port is blocked or unblocked.
- **Beaconing** — This field indicates the beaconing status for the port.
- **FAN Configuration** — This field indicates the FAN status for the port. This field is valid only on the Edge Switch 2/24.
- **Operational State** — Inactive, invalid attachment, link incident, no light, not operational, online, offline, port failure, segmented E_Port, testing, or not installed.
- **Reason** — When the port operating state is Segmented E_Port, Invalid Attachment, or Inactive, this field displays the reason for that state. When an E_Port is segmented, two fabrics are prevented from joining. This only occurs when the switch is attempting to connect to another switch. Reasons and probable causes are as follows:
  - — If Operational State is Segmented E Port:
    - — Segment Not Defined
    - — Incompatible Operating Parameters
    - — Duplicate Domain ID(s)
    - — Incompatible Zoning Configurations
    - — Build Fabric Protocol Error

- No Principal Switch
- No Response from Attached Switch
- ELP Retransmission Failure Timeout

— If Operational State is `Invalid Attachment`:

- Unknown
- ISL connection not allowed on this port
- ELP rejected by the attached switch
- Incompatible switch at other end of the ISL
- External loopback adapter connected to the port
- N_Port connection not allowed on this port
- Non-HP high availability fabric switch or compatible switch at other end of the ISL
- ISL connection not allowed to external Fabrics
- Port binding violation — unauthorized WWN
- Unresponsive node connected to Port

— If Operational State is `Inactive`:

- No Serial Number
- No Key Enabled
- Switch Speed Conflict
- Optics Speed Conflict (Director 2/64 and Director 2/140 only)
- No SBAR Support (Director 2/64 and Director 2/140 only)

■ **Technology**

Identifies the technology used for the following aspects of the port:

— **Connector Type** — The type of connector: `LC`, `MT_RJ`, `MU`, `Unknown`, or `Internal Port`.

— **Transceiver** — The type of transceiver: `Longwave Laser (LC)`, `Shortwave Laser`, `Shortwave Laser with OFC`, `Longwave Laser (LL)`, `Long Distance Laser`, `Unknown`, or `None`.

— **Distance Capability** — General distance range for port transmission: `Short`, `Intermediate`, `Long`, `Very Long`, or `Unknown`.

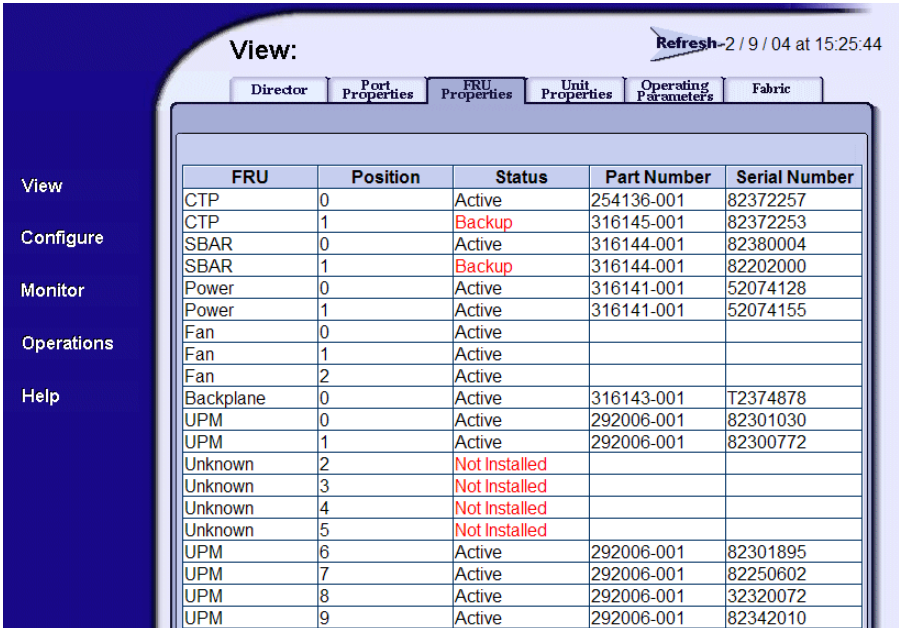
— **Media** — The Fibre Channel mode and optic size: `Single-Mode`, `Multi-Mode 50 micrometer`, `Multi-Mode 62.5 micrometer`, `Multi-Mode 50`, `62.5 micrometer`, or `Unknown`.

— **Speed** — The speed capability of the product. Values that may display include `1 Gb/s`, `2 Gb/s`, and `Unknown`. Both `1 Gb/s` and `2 Gb/s` may display for optics that support both speeds.

Viewing FRU Properties

To view the properties of an FRU on a product, perform the following procedure:

1. Choose **View** from the navigation panel.
2. Choose the **FRU Properties** tab. The **FRU Properties** tab view displays (Figure 28) showing each FRU on the product.



FRU	Position	Status	Part Number	Serial Number
CTP	0	Active	254136-001	82372257
CTP	1	Backup	316145-001	82372253
SBAR	0	Active	316144-001	82380004
SBAR	1	Backup	316144-001	82202000
Power	0	Active	316141-001	52074128
Power	1	Active	316141-001	52074155
Fan	0	Active		
Fan	1	Active		
Fan	2	Active		
Backplane	0	Active	316143-001	T2374878
UPM	0	Active	292006-001	82301030
UPM	1	Active	292006-001	82300772
Unknown	2	Not Installed		
Unknown	3	Not Installed		
Unknown	4	Not Installed		
Unknown	5	Not Installed		
UPM	6	Active	292006-001	82301895
UPM	7	Active	292006-001	82250602
UPM	8	Active	292006-001	32320072
UPM	9	Active	292006-001	82342010

Figure 28: FRU Properties tab view

This page shows the following information for the FRUs:

- **FRU** — Name of the FRU.
- **Position** — Slot position relative to identical FRUs installed in the chassis.

- **Status** — Status of the FRU: `Active`, `Backup`, `Failed`, or `Not Installed`.
- **Part number** — The OEM part number, as set in non-volatile memory of the FRU (if applicable).
- **Serial number** — Serial number of the FRU, as set in its non-volatile memory (if applicable).

Viewing Unit Properties

To view the unit properties of a product, perform the following procedure:

1. Choose **View** from the navigation panel.
2. Choose the **Unit Properties** tab. The **Unit Properties** tab view displays (Figure 29) showing product properties.

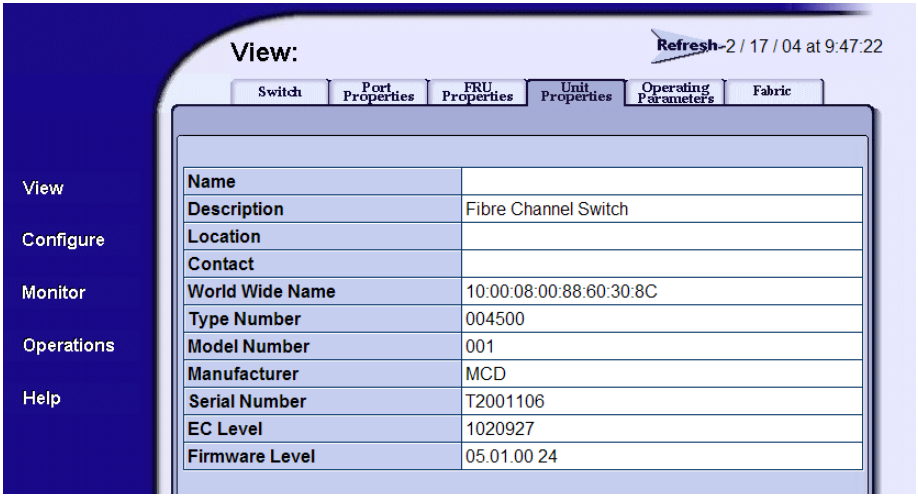


Figure 29: Unit Properties tab view

This page shows the following information for the product:

- **Name** — The name configured for the port.
- **Description** — A configurable description of the product functionality.
- **Location** — Location of the product.
- **Contact** — Name of the product's point of contact.
- **WWN** — Fibre Channel WWN address.

- **Type Number** — Type Number of the product (such as 6064 for the Director 2/64).
- **Model Number** — Model Number of the product.
- **Manufacturer** — Three-letter identifier of the product's manufacturer.
- **Serial Number** — Product serial number.
- **EC Level** — Current engineering change (EC) level.
- **Firmware Level** — Release number of the firmware that is currently installed.

Viewing Operating Parameters for the Product

To view the Operating Parameters of a product, perform the following procedure:

1. Choose **View** from the navigation panel.
2. Choose the **Operating Parameters** tab. The **Operating Parameters** tab view displays (Figure 30) showing **Switch Parameters** and **Fabric Parameters**.

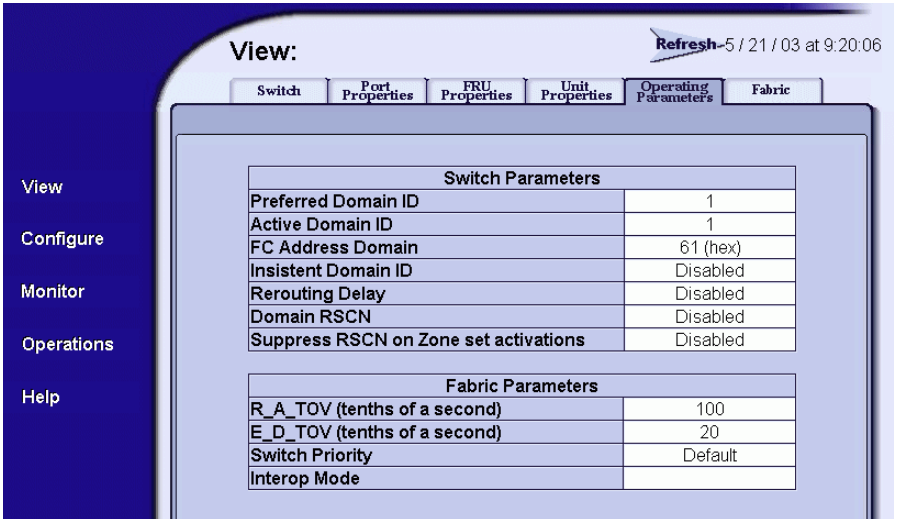


Figure 30: Operating Parameters tab view

This tab view shows the following **Switch Parameters** information for the product:

- **Preferred Domain ID** — The ID to be used if the product participates in a multiswitch fabric. The preferred domain ID must be unique for each director and switch in a fabric.
- **Active Domain ID** — The domain ID assigned to the switch.
- **FC Address Domain ID** — The value of the domain byte of the Fibre Channel address for ports on this product.
- **Insistent Domain ID** — Indicates whether the domain ID is enabled to be insistent. This option is required if Enterprise Fabric Mode (an optional SANtegrity Binding feature) is enabled.
- **Rerouting Delay** — Indicates whether rerouting delay is enabled. Enabling the rerouting delay ensures that frames are delivered in order through the fabric to their destination.
- **Domain RSCN** — Domain Register For State Change Notifications (domain RSCNs) are sent between end devices in a fabric to provide additional connection information to host bus adapters (HBA) and storage devices. This option is required if Enterprise Fabric mode (an optional SANtegrity feature) is enabled.
- **Suppress RSCN on Zone Set Activiations** — If enabled, registered state change notification (RSCN) messages are prohibited from being sent to ports on the switch following any change to the fabric's active zone set. If the state shown is disabled, RSCN messages are sent to ports on the switch for changes to the fabric's active zone set.
- **Operating Mode** — Indicates whether the operation mode is S/390 mode or Open Systems mode. (S/390 mode is not supported with the Edge Switch 2/24.)

Note: The operation mode parameter of the EWS interface is equivalent to the management style parameter of the HAFM interface. The S/390 mode used for the EWS interface is equivalent to the FICON management style on the HAFM. The EWS term Open Systems mode is equivalent to Open Systems management style for the HAFM.

- **Director Speed** — speed of communications on the product. Values can be 1 Gb/s or 2 Gb/s. Valid on the Director 2/64 only.

Viewing Fabric Information

Options on the **View** panel of the EWS interface enable you to see information about the fabric in which a product participates. You can view each of the following:

- Operating parameters for a fabric.
- Information about each of the devices that make up the fabric.
- Topology of the fabric.

Viewing Operating Parameters for a Fabric

To view the Operating Parameters of a product, perform the following procedure:

1. Choose **View** from the navigation panel.
2. Choose the **Operating Parameters** tab. The **Operating Parameters** tab view displays (Figure 30) showing **Switch Parameters** and **Fabric Parameters**.

This tab view shows the following **Switch Parameters** information for the product:

- **BB Credit** — the BB_Credit value for the fabric (not available on the Edge Switch 2/24).
- **R_A_TOV** — Resource Allocation Time Out Value (R_A_TOV) used by the fabric. Specified in tenths of a second.
- **E_D_TOV** — Error Detection Time Out Value (E_D_TOV) value used by the fabric. Specified in tenths of a second.
- **Switch Priority** — Priority value of the switch. Values can be `Default`, `Principal`, and `Never Principal`.
- **Interop Mode** — Interoperability mode of the fabric. Values can be **Homogenous Fabric** and **Open Fabric 1.0**. (This field is not valid if the product's Operation Mode is **S/390**.)

Viewing Fabric Directors and Switches

To view information about the HP high availability fabric directors and switches on a menu, perform the following procedure:

1. Choose **View** from the navigation panel.
2. Choose the **Fabric** tab and the **Products** tab. The **Products** tab view displays (Figure 31).

Note: The page may take some time to display. If the message `Attempting to Collect Data` displays in a product cell, you may want to refresh the image to load data that has been collected. Click the **Refresh** icon at the top right of the window.

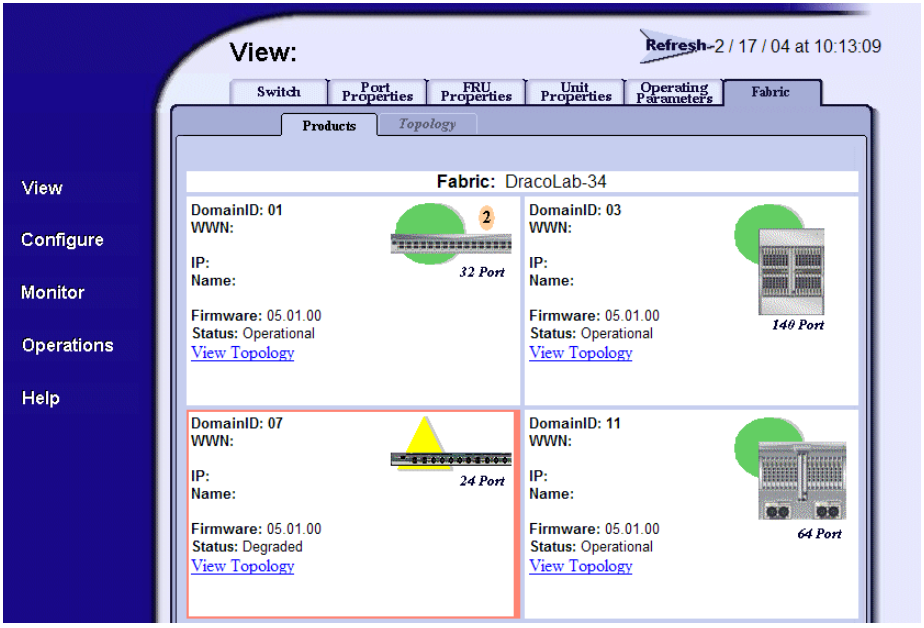


Figure 31: Fabric tab with Products tab view

The **Products** page provides a quick glance at the devices in the fabric, as well as direct hyperlink access to fabric participants that support the EWS interface. The devices are shown in separate product cells organized by domain ID in numerical order.

Each device on the fabric is shown in a separate box called a product cell. The boxes consist of a list of properties for the device, and a graphic showing the product and a symbol that represents the status of the product.

The information shown in the product cells reflects the state of devices before the information displays. This information does not update automatically. You must refresh the screen manually to see the most recent information. Click the **Refresh** icon at the top right of the window.

Note: If the message `Attempting to Collect Data` displays in a product cell, you may want to reload the page, because it will not update automatically after the initial view is loaded.

Parts of the Product Cell

The product cell has the following parts:

- A graphic representation of the device and its status. For more information, see "Parts of the Product Graphic" on page 113.
- Information about the device. For more information, see "Product Cell Information" on page 112
- **View Topology** text that acts as a hyperlink to the **Topology** page for the fabric (firmware 04.00.00 and higher only). Choose this hyperlink to view the **Topology** page. (The hyperlink is found only on the Edge Switch 2/16, Edge Switch 2/32, Edge Switch 2/24, SAN Director 64, Director fc-64, Director 2/64, and Director 2/140.) Other HP switches and non-HP products do not have this hyperlink.

Product Cell Information

Each product cell provides information about a device on the fabric as described in Table 6.

Table 6: Information on the Product Cell

Information	Description	Availability
Domain ID	Domain ID of the product used in the fabric.	Available for any product.
WWN	WWN of the product used in the fabric.	Available for any product.
IP	IP addresses of the product.	HP high availability fabric directors and switches only.

Table 6: Information on the Product Cell

Information	Description	Availability
Name	Nickname assigned to the product.	HP high availability fabric directors and switches only.
Firmware	Level of firmware used by the product.	HP high availability fabric directors and switches only.
Status	Status of the product, which can be **Operational**, **Degraded**, **Failed**, **or Unknown**.	The following HP high availability fabric directors and switches only: ■ Edge Switch 2/12 ■ Edge Switch 2/16 ■ Edge Switch 2/32 ■ Edge Switch 2/24 ■ SAN Director 64 ■ Director fc-64 ■ Director 2/64 ■ Director 2/140

Parts of the Product Graphic

The product graphic provides the following information:

- The maximum number of ports on the product.
- A graphic representing the status of the product.
- An icon representing the appearance of the product. You can click the graphic to view the default pages for these devices:
  - Edge Switch 2/12
  - Edge Switch 2/16
  - Edge Switch 2/24
  - Edge Switch 2/32
  - SAN Director 64
  - Director fc-64
  - Director 2/64
  - Director 2/140

— Generic product. All other HP products in the fabric have a generic product graphic. The generic product graphic does not provide a link to the device's default page.

The symbols that display behind the product graphic indicate the status of the product. The meaning of each symbol is explained in Table 7.

Table 7: Operating Status Symbols

Symbol	Symbol Name	Status	Meaning
	Green Circle	Fully Operational	All components and installed ports are operational; no failures.
	Yellow Triangle	Redundant Failure	A redundant component has failed, such as a power supply, and the backup component has taken over operation.
		Minor Failure	A failure occurred that has decreased the product's operational ability. Normal switching operations are not affected. One or more ports failed, but at least one port is still operational. A fan has failed or is not rotating sufficiently.
	Red Diamond	NOT OPERATIONAL	A critical failure prevents the product from performing fundamental operations. All fans failed. All installed ports failed. Both power supplies failed.

Viewing Fabric Topology

The topology of a fabric is a high-level view of the routing and pathways on the fabric. To view the fabric topology from the viewpoint of the hosting machine, perform the following procedure:

1. Choose **View** from the navigation panel.

2. Choose the **Fabric** tab and the **Topology** tab. The **Topology** tab view displays (Figure 32).

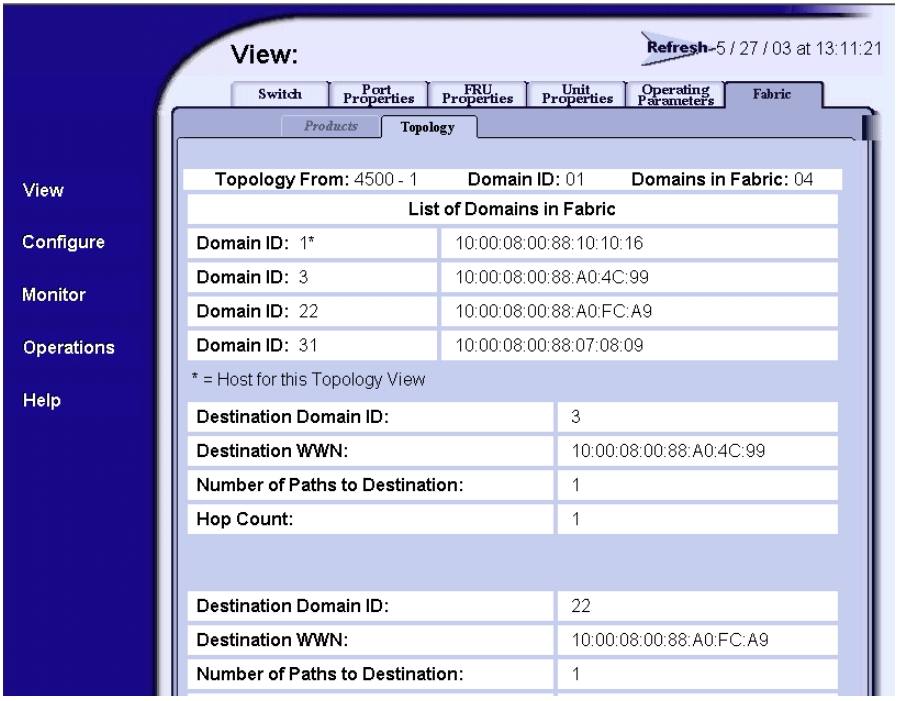


Figure 32: Fabric tab with Topology tab view

Note: If you attempt to access this page during a fabric build, or any other instance in which the fabric is not operational, only the top line of the page displays, with the message `Fabric Not Operational`.

---

3. The **Topology** page provides the information shown in Table 8.

Table 8: Components of the Topology Page

Part of Page	Component	Description
Host Information	Topology From	Identifies the host product that is providing the fabric topology information. All information on the page is provided from the point of view of the host machine.
	Domain ID	Domain ID of the host product.
	Domains in Fabric	The total number of domains in the fabric.
List of Domains in Fabric	Domain ID	Domain IDs of each device in the fabric. (The ID number that is followed by an asterisk is the ID for the host product.)
	WWN	WWN of the device that corresponds to the Domain ID next to the WWN.
Destination Description	Destination Domain ID	The Domain ID of the destination device. The destination device is described from the point of view of the host product.
	WWN	WWN of the destination device.
	Number of Paths to Destination	Total paths that can be used by the host product to communicate with the destination device.
	List of Paths	A list of each path used by the host product to communicate with the destination device. The details include the Exit Port used for the path and the number of hops needed to reach the destination fabric device.

Monitoring Products

5

The **Monitor** page is used to access information about the product including port and node information as well as critical information about performance. Key tasks you can perform to troubleshoot problems from the **Monitor** page are:

Monitoring Ports

You can obtain information about ports from the **Port List** and **Port Stats** tab views.

Port List

Choose **Monitor** on the navigation panel. The **Port List** tab view displays (Figure 33). The **Port List** tab view provides the following information including information on the port state:

- **Port #** — The number of the port.
- **Name** — Displays the port name as configured through the **Configure Ports** tab.
- **Block Configuration** — Indicates the blocked or unblocked configuration of the port:
  - `Blocked` — Devices communicating with the port are prevented from logging into the product or communicating with other devices attached to product ports.
  - `Unblocked` — Devices communicating with the port can log in to the product and communicate with devices attached to any other unblocked port in the same zone.
- **State** — See "Port Operational States" on page 119 for an explanation of the states.
- **Type** — The type of port. The valid options vary by product.

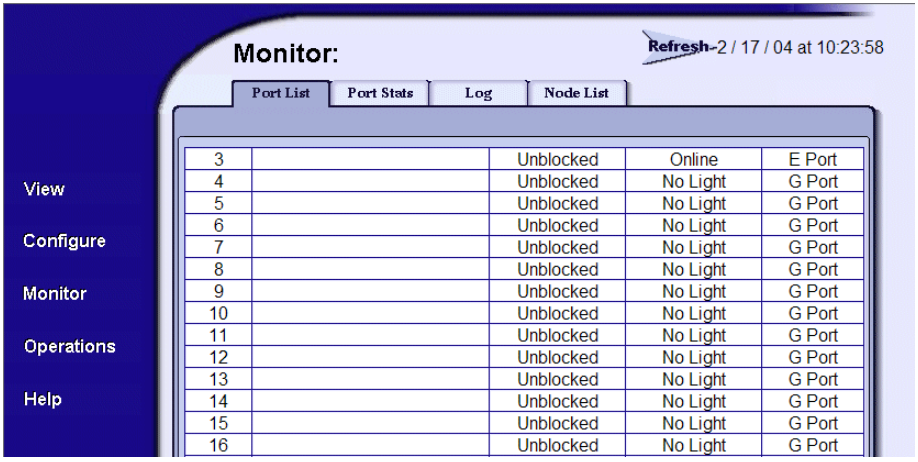


Figure 33: Port List tab view

Port Operational States

The **State** column of the **Port List** tab view displays one of the following operational states:

- `Beaconing` — The port is beaconing, which means that the beaconing light is flashing on the physical hardware. (A port in a failed state cannot beacon.)
- `Inactive` — The switch port is in an inactive state. Reasons for this state display in the **Reason** field of the **Port Properties** page. (See "Viewing Port Properties" on page 102 for more information.)

Note: Note that if port optics have also failed, the amber LED will be on.

- `Invalid Attachment` — The switch port is in an invalid attachment state.
- `Link Incident` — A link incident occurred on one of the ports.
- `Link Reset` — The switch and the attached device are performing a link reset operation to recover the link connection. Ordinarily, this is a transient state.
- `No Light` — No signal (light) is being received on the switch port. This is a normal condition when there is no cable plugged into the port or when the power of the device attached to the other end of the link is off.

- `Not installed` — The port optics are not installed or the feature that provides additional port function is not enabled.
- `Not Operational` — The switch port is receiving the Fibre Channel not operational sequence (NOS) indicating that the attached device is not operational.
- `Online` — The attached device has successfully connected to the switch and is ready to communicate or is in the process of communicating with other attached devices.
- `Offline` — The switch port was configured as “blocked” and is transmitting the Fibre Channel OLS to the attached device.
- `Port Failure` — The switch port has failed and requires service. (A port in the failed state cannot beacon.)
- `Segmented E_Port` — The E_Port is segmented preventing the two fabrics from joining (this only occurs when two switches are connected to each other).
- `Testing` — Port is executing an internal loopback test.

Accessing Port Statistics

Choose **Monitor** on the navigation panel. Choose the **Port Stats** tab; the **Port Stats** tab view displays (Figure 34).

To display port statistics for a selected port, enter a port number in the **Port Number** field and choose **Get Port Statistics**. (You can also choose the **Back** or **Fwd** buttons to view the previous or next port.) The Port Statistics are divided into Traffic Statistics, Error Statistics, Class Two Statistics, and Class Three Statistics. (You may need to scroll down to see all of the categories.)

The information shown that displays is current as of the time when the view displays. The information does not update automatically.

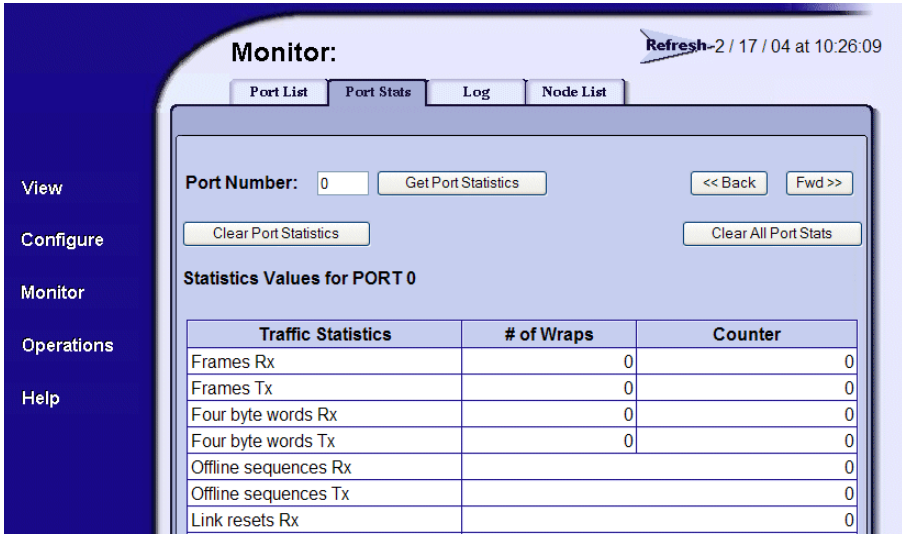


Figure 34: Port Statistics tab view

Troubleshooting Tip for Port Stats

As a general rule, you should clear all the counters by choosing **Clear Port Stats** or **Clear All Port Stats** after you have resolved a problem. When troubleshooting, keep track of the time interval when errors accumulate to judge the presence and severity of a problem. (There is a link recovery hierarchy implemented in Fibre Channel to handle some level of "expected anomalies.") For troubleshooting purposes, you want to focus on errors that, as displayed in the **Counter** column, increment very quickly.

Parts of Statistics Tables

The tables of statistics contain the following columns:

- **Statistics** — Type of statistic being tracked.
- **# of Wraps** — Number of times the **Counter** value wraps, for statistics that grow rapidly. The maximum value that either the **Counter** or the **# of Wraps** can hold is 2^{32}, or 4,294,967,296. Each time the **Counter** field reaches the maximum value of 2^{32}, the wrap count is incremented by 1.
- **Counter** — Number of instances of the tracked item recorded since system initialization or the last time the counters were cleared.

Traffic Transmit and Receive Statistics

The Traffic Statistics include these transmit and receive values.

- **Frames Rx** — Number of frames that the port has received.
- **Frames Tx** — Number of frames that the port has transmitted.
- **Four byte words Rx** — Number of words that the port has received.
- **Four byte words Tx** — Number of words that the port has transmitted.
- **Offline sequences Rx** — Number of offline sequences (OLS) received by this port.
- **Offline sequences Tx** — Number of offline sequences (OLS) transmitted by this port.
- **Link resets Rx** — Number of link reset protocol frames received by this port from the attached N_Port.
- **Link resets Tx** — Number of link reset protocol frames transmitted by this port to the attached N_Port.
- **Link utilization % Rx** — Current link utilization for the port expressed as a percentage. On 1 Gb/s links, ports can transmit or receive data at 100 MB per second. On 2 Gb/s links, ports can transmit or receive data at 200 MB per second. Link utilization is calculated over one-second intervals.
- **Link utilization % Tx** — Current link utilization for the port expressed as a percentage. On 1 Gpbs links, ports can transmit or receive data at 100 MB per second. On 2 Gb/s links, ports can transmit or receive data at 200 MB per second. Link utilization is calculated over one-second intervals.

For the Edge Switch 2/24, the following statistics are also shown:

- **LIPs Detected** — A loop initialization primitive (LIP) was detected, which means the loop was completed.
- **LIPs Generated** — A loop initialization primitive was created to initialize a loop.

Error Statistics

The Error Statistics include these transmit and receive values:

- **Link failures** — Number of link failures recorded because a not operational sequence (NOS), protocol timeout, or port failure was detected.
- **Sync losses** — Number of loss-of-synchronizations detected because an attached device was reset or disconnected from the port.
- **Signal losses** — Number of loss-of-signal errors detected because the attached device was reset or disconnected from the port.
- **Primitive sequence errors** — Number of primitive sequence protocol errors received from an attached device, which indicates a Fibre Channel link-level protocol violation.
- **Discarded frames** — A received frame could not be routed and was discarded because the frame timed out due to an insufficient buffer-to-buffer credit, or the destination device was not logged into the product.
- **Invalid transmission words** — Number of invalid transmission words from an attached device. This indicates that a frame or primitive sequence arrived at the port corrupted.
- **CRC errors** — A received frame failed a cyclic redundancy check (CRC) validation, indicating the frame arrived at the port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber cable, or a poor cable connection.
- **Delimiter errors** — Number of times that the switch detected an unrecognized start-of-frame (SOF), an unrecognized end-of-frame (EOF) delimiter, or an invalid class of service. This indicates that the frame arrived at the switch's port corrupted. This corruption can be due to plugging/unplugging the link, bad optics at either end of the cable, bad cable, or dirty or poor connections. Moving the connection around or replacing cables can isolate the problem.
- **Address ID errors** — A received frame had an unavailable or invalid Fibre Channel destination address, or an invalid Fibre Channel source address. This typically indicates the destination device is unavailable.

- **Frames too short** — A received frame exceeded the Fibre Channel frame maximum size or was less than the Fibre Channel minimum size, indicating the frame arrived at the switch's port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber cable, or a poor cable connection.

Class 2 Statistics

The Class 2 Statistics include these transmit and receive values:

- **Received Frames** — Number of Class 2 frames received by this F_Port from its attached N_Port.
- **Transmitted Frames** — Number of Class 2 frames transmitted by this F_Port to its attached N_Port.
- **Busied Frames** — Number of F_BSY frames generated by this F_Port against Class 2 frames.
- **Rejected Frames** — Number of F_RJT frames generated by this F_Port against Class 2 frames.
- **4-byte words Rx** — Number of Class 2, 4-byte words received by the port.
- **4-byte words Tx** — Number of Class 2, 4-byte words transmitted by the port.

Class 3 Statistics

The Class 3 Statistics include these transmit and receive values:

- **Received Frames** — Number of Class 3 frames received by the F_Port from its attached N_Port.
- **Transmitted Frames** — Number of Class 3 frames transmitted by this F_Port to its attached N_Port.
- **Discarded Frames** — Number of Class 3 frames discarded (including multicast frames with bad Domain IDs).
- **4-byte words Rx** — Number of Class 3, 4-byte words received by the port.
- **4-byte words Tx** — Number of Class 3, 4-byte words transmitted by the port.

Open Trunking Statistics

The Open Trunking Statistics include these transmit and receive values:

- **Flows rerouted to ISL** — The number of Fibre Channel traffic flows that were rerouted to this ISL from another ISL due to congestion. (This value increments only if the Open Trunking feature is installed.)

- **Flows rerouted from ISL** — The number of Fibre Channel traffic flows that were rerouted from this ISL to another ISL due to congestion. (This value increments only if the Open Trunking feature is installed.)

Viewing Logs

Select **Monitor** on the navigation panel. Select the **Logs** tab; the **Log*s*** tab view displays (Figure 35).

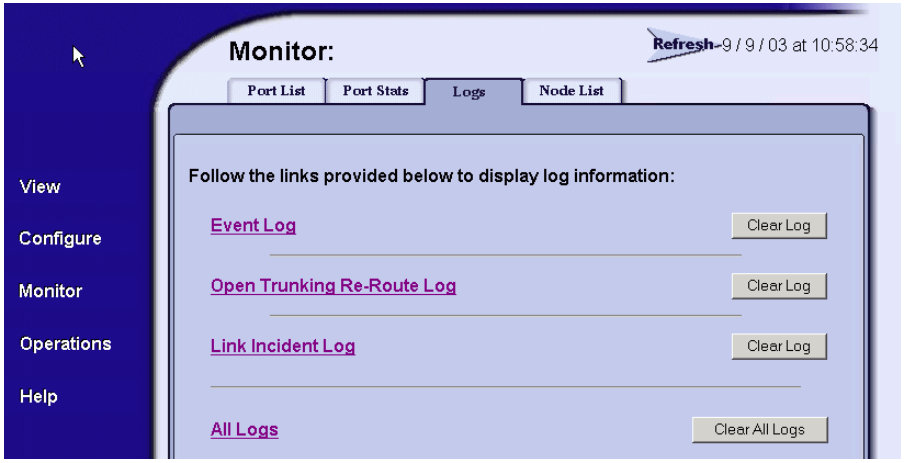


Figure 35: Logs Tab View

The **Logs** tab provides links to the following logs:

- Event Log — A listing of messages generated by the product regarding errors and events. The four levels of events indicate an increasing level of severity, from Informational to Severe. For more information, see "Viewing the Event Log" on page 127.
- Open Trunking Re-Route Log — A log of open trunking re-route actions made by the product. For more information, see "Viewing the Open Trunking Re-Route Log" on page 129.
- Link Incident Log — A log of link incidents that have occurred. For more information, see "Viewing the Link Incident Log" on page 131.
- All Logs — collects the information for each of the three logs into a single text page. For more information, see "Viewing All Logs" on page 133.

Each log contains a link that brings the user to a page of ASCII text that reflects the log information present on the machine at that moment. The log displayed is a snapshot of the current log information. Log entries are displayed in the order in which they occurred, with most recent entries listed first. Each log also contains a **Clear Log** button that is used to clear all the entries in the log.

Viewing the Event Log

Select **Monitor** on the navigation panel. Select the **Logs** tab; the **Logs** tab view displays. Select the **Event Log** link. The Event Log displays in text format, as shown in Figure 36. The log displays in a separate browser window. Close the browser window to close the log.

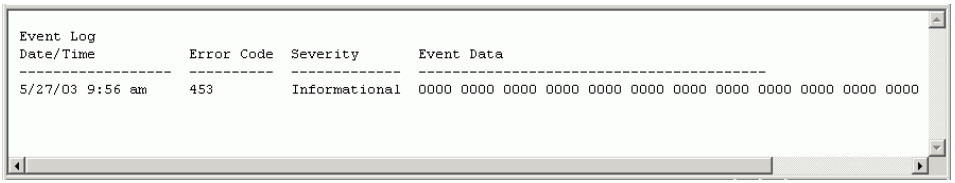


Figure 36: Event Log Viewer

The Event Log displays a record of significant events that have occurred on the product, such as degraded operation, FRU failures, and port problems. The Event Log is an important tool you can use to monitor and troubleshoot the products in the SAN. Information contained in the event log may also be used by customer support and service personnel to help resolve problems.

The Event Log displays the following information:

- Date/Time — Represents the date and time the event occurred on the switch.
- Error code — Numeric code for the event. For more information, see "Error Event Code Categories" on page 127.
- Severity — The severity of the event represented in text. There are four levels, indicating an increasing level of severity: Informational, Minor, Major, and Severe (not operational).
- Event Data — Hexadecimal data provided with the event.

Error Event Code Categories

Error Event Codes define event categories; the categories and events vary by product. Below is a list of event codes:

- 1xx — system events
- 2xx — power supply events
- 3xx — fan events
- 4xx — control processor card events

- 5xx — port or universal port module card events
- 6xx — serial crossbar assembly (SBAR) events
- 8xx — thermal incident events

For detailed information on event codes and isolating problems from event data, refer to the product installation and service manual.

Note: In addition to the event log, another method to obtain operation information about the status of the product is from the Fabric tab view. Refer to "Viewing Product and Fabric Data" on page 99.

Clearing Event Log Entries

Note: Before clearing logs, make sure the logs are not needed for troubleshooting. Once a log is cleared, the data cannot be retrieved.

To clear the Event Log, select **Monitor** and select the **Logs** tab. Select the **Clear Log** button, next to the Event Log link. A message displays stating that the operation has been performed successfully.

Viewing the Open Trunking Re-Route Log

Select **Monitor** on the navigation panel. Select the **Logs** tab; the **Logs** tab view displays. Select the **Open Trunking Re-Route Log** link. The Open Trunking Re-Route Log displays in text format, as shown in Figure 37. The log displays in a separate browser window. Close the browser window to close the log.

Note: Open Trunking is a licensed feature. This log does not contain data unless the Open Trunking feature key is installed and enabled, and the system has performed re-routing.

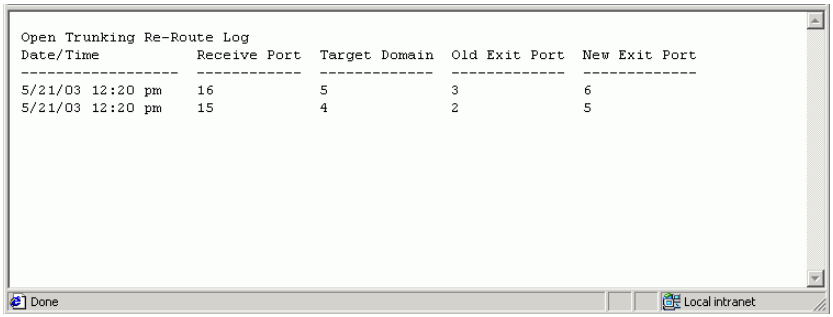


Figure 37: Open Trunking Re-Route Log View

The Open Trunking feature monitors the average data rates of all traffic flows on InterSwitch Links (ISLs) and periodically reroutes data flows from congested links to lightly loaded links. These rerouting activities are recorded in the Open Trunking Re-Route Log.

The Open Trunking Re-Route Log provides the following:

- Date/Time — Date and time when rerouting occurred.
- Receive Port — The decimal receive-port number on the local switch associated with the flow that was rerouted.
- Target Domain — The decimal domain ID associated with the flow that was rerouted.
- Old Exit Port — The decimal exit-port number on this switch that the flow used to use to get to the target domain.
- New Exit Port — The decimal exit port number on this switch that the flow now uses to get to the target domain.

Clearing Open Trunking Re-Route Log Entries

Note: Before clearing logs, make sure the logs are not needed for troubleshooting. Once a log is cleared, the data cannot be retrieved.

To clear the Open Trunking Re-Route Log, select **Monitor** and select the **Logs** tab. Select the **Clear Logs** button, next to the Open Trunking Re-Route Log link. A message displays stating that the operation has been performed successfully.

Viewing the Link Incident Log

Select **Monitor** on the navigation panel. Select the **Logs** tab; the **Logs** tab view displays. Select the **Link Incident Log** link. The Link Incident Log displays in text format, as shown in Figure 38. The log displays in a separate browser window. Close the browser window to close the log.

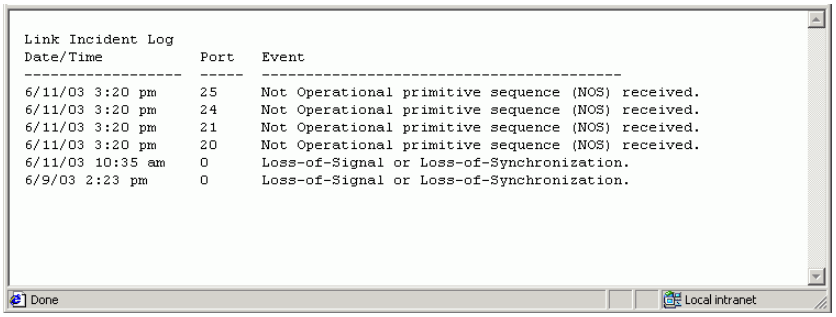


Figure 38: Link Incident Log View

The Link Incident Log provides the following information about link incidents:

- Date/Time — Date and time when the link incident event occurred.
- Port — The port on which the link incident occurred.
- Link Incident Event — An ASCII string describing the link incident event. The following events may cause a link incident to be written to the log:
  - — Implicit incident. The attached node detects a condition that may cause problems on the link.
  - — Bit-error threshold exceeded. The number of code violation errors has exceeded the specified threshold.
  - — Loss-of-signal or Loss-of-synchronization. This occurs if a cable is unplugged from an attached node. Loss-of-signal occurs when a cable is unplugged from an attached node. Loss-of-synchronization is reported if the condition has persisted for longer than the resource allocation time out value (R_A_TOV).
  - — Not-operational (NOS) primitive sequence received.
  - — ------Primitive sequence timeout:
  - — ------Link reset protocol timeout occurred.

— Timeout occurred for an appropriate response while in NOS receive state and after NOS is no longer recognized.

- Invalid primitive sequence received for the current link state. Either a link reset or a link reset response primitive sequence was recognized while waiting for the offline sequence.

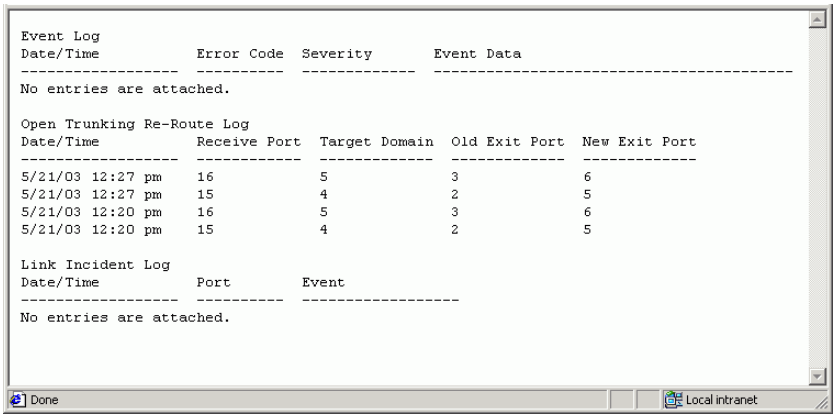
Clearing Link Incident Log Entries

Note: Before clearing logs, make sure the logs are not needed for troubleshooting. Once a log is cleared, the data cannot be retrieved.

To clear the Link Incident Log, select **Monitor** and select the **Logs** tab. Select the **Clear Log** button, next to the Link Incident Log link. A message displays stating that the operation has been performed successfully.

Viewing All Logs

Select **Monitor** on the navigation panel. Select the **Logs** tab; the **Logs** tab view displays. Select the **All Logs** link. The All Logs listing displays in text format, as shown in Figure 39. The log displays in a separate browser window. Close the browser window to close the log.



```
Event Log
Date/Time           Error Code  Severity       Event Data
------------------  ----------  -------------  ----------------------------------------
No entries are attached.

Open Trunking Re-Route Log
Date/Time           Receive Port  Target Domain  Old Exit Port  New Exit Port
------------------  ------------  -------------  -------------  -------------
5/21/03 12:27 pm    16            5              3              6
5/21/03 12:27 pm    15            4              2              5
5/21/03 12:20 pm    16            5              3              6
5/21/03 12:20 pm    15            4              2              5

Link Incident Log
Date/Time           Port        Event
------------------  ----------  ------------------
No entries are attached.
```

Done | Local intranet

Figure 39: All Logs View

The All Logs listing provides the complete content of the following logs:

- Event Log — For more information, see “Viewing the Event Log” on page 127.
- Open Trunking Re-Route Log — For more information, see “Viewing the Open Trunking Re-Route Log” on page 129.
- Link Incident Log — For more information, see “Viewing the Link Incident Log” on page 131.

Clearing All Log Entries

Note: Before clearing logs, make sure the logs are not needed for troubleshooting. Once the logs are cleared, the data cannot be retrieved.

To clear all logs’ entries, select **Monitor** and select the **Logs** tab. Select the **Clear All Logs** button, next to the All Logs link. A message displays stating that the operation has been performed successfully.

Viewing Node List

Choose **Monitor** on the navigation panel. Choose the **Node List** tab; the **Node List** tab view displays (Figure 40). The **Node List** tab view displays information about all node attachments or N_Ports that have logged into existing F_Ports on the product. All data is dynamically updated as the nodes log in and log out. To update the information in the view, click the **Refresh** button.

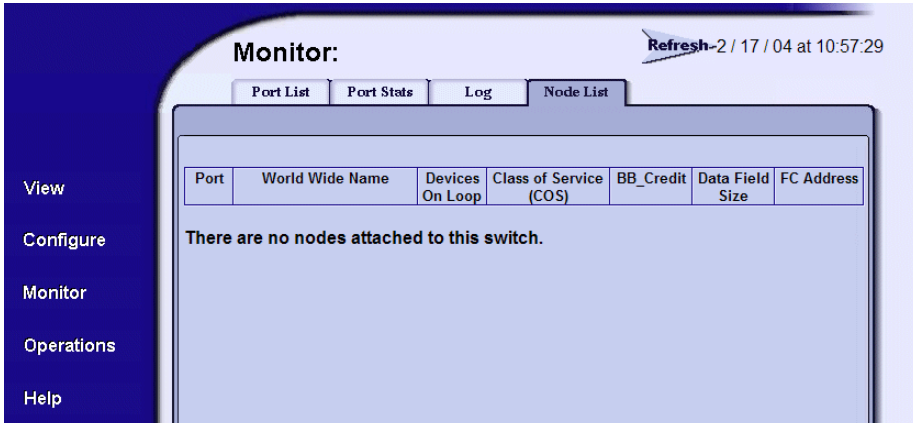


Figure 40: Node List tab view

Information displayed for each node includes:

- **Port** — Port number.
- **World Wide Name** — The 16-digit WWN assigned to the attached node.
- **Class of Service (COS)** — Class 2 and/or Class 3 service.
- **BB_Credit** — Buffer-to-buffer credit the attached node has available.
- **Data Field Size** — Largest Fibre Channel frame the node can process.

For the Edge Switch 2/12 and 2/24, these values are also displayed:

- **Devices on Loop** — Number (device count) of public and private loop-attached devices. This field entry contains a hyperlink to a screen that shows a list of devices on a loop for the port. This tab view shows the **FC Address**, **WWN**, **COS**, and **Data Field Size** for each device in the loop.
- **FC Address** — Fibre Channel address, which is shown only if there is a single attached device on the loop. Otherwise, all Fibre Channel address information is displayed on the port-specific page.

Operating and Managing Products and Parts

6

The **Operations** page is used to manage the product and ports as well as perform maintenance tasks such as port diagnostics. You can access information and tools that are useful in troubleshooting from the **Operations** page. Key tasks you can perform to troubleshoot problems from the **Operations** page are:

Setting Product Beaconing On or Off

Choose **Operations** from the navigation panel. The **Switch** or **Director** tab displays, depending on the type of product. Choose the **Beacon** tab; the **Beacon** tab view displays (Figure 41).

Using this view, you can enable or disable beaconing on the product. The current state of beaconing for the unit, which is either on or off, is displayed by a flashing LED. Beaconing is useful in helping to isolate problems and locate the product, especially when there are multiple HP high availability fabric directors and switches stacked together, such as in a rack-mount cabinet.

You can change the beaconing state from on or off by choosing **Activate**. For example, if the page displays **Unit beaconing is Off**, choosing **Activate** will turn beaconing on. After you refresh the web browser, by choosing the **Beacon** tab, the page will then display **Unit Beaconing is On**.

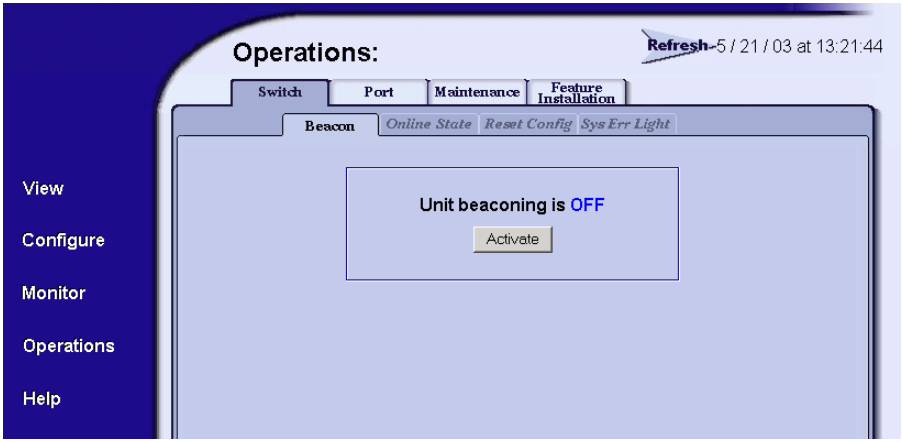


Figure 41: Setting product beaconing

Setting Product Online or Offline

Choose **Operations** from the navigation panel. Choose the **Switch** or **Director** tab as appropriate. Choose the **Online State** tab; the **Online State** tab view displays (Figure 42).

A box displays with the current online state and a button that is used to change the state of the product.

If the state of the product is online, the tab view indicates that the current state is online. Click the **Set Offline** button to set the product offline.

If the state of the product is offline, the tab view indicates that the current state is offline. Click the **Set Online** button to set the product online.

If your changes are successful a message displays stating that your changes have been successfully activated. You can refresh the web browser to verify the change has been made.

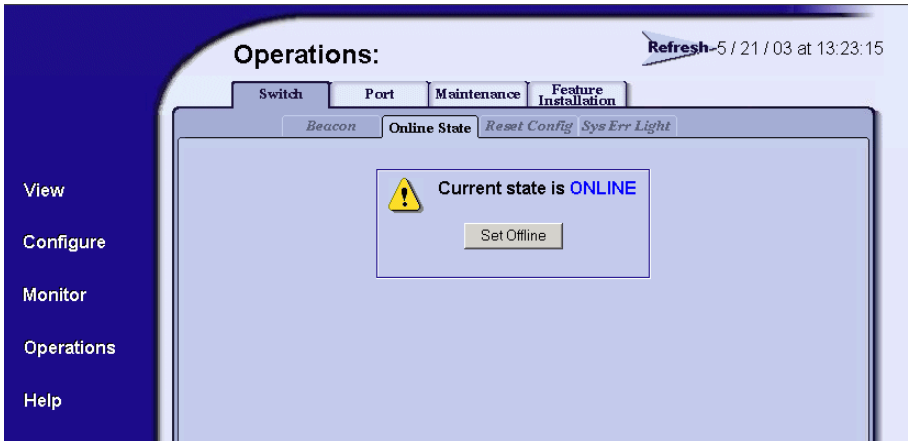


Figure 42: Setting product online or offline

Resetting Product Configuration to Default Values

Choose **Operations** from the navigation panel. Choose the **Switch** or **Director** tab as appropriate. Choose the **Reset Config** tab; the **Reset Config** tab view displays (Figure 43). You can use this view to reset product configuration values. This enables you to reset all configuration data and nonvolatile settings to the factory default values including any data that was created from the **Configure** page and associated tabs.

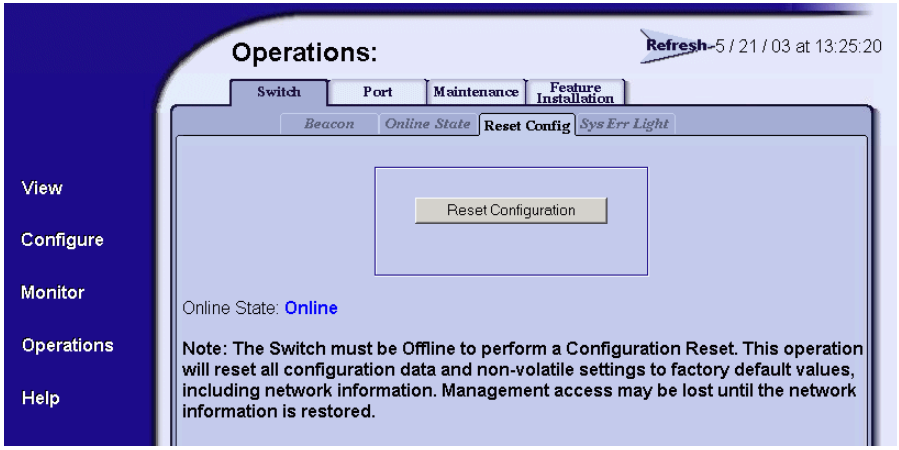


Figure 43: Resetting product to default values

Note: You may be asked by service personnel to perform this operation to resolve system problems. Be sure to review the information in this section completely before performing this operation.

For a list of factory default values, refer to the product's installation and service manual.

Caution: This operation will reset all configuration data and non-volatile settings to the factory default values. All optional features will also be disabled. You will need to activate optional features after completing the product reset.

Note: Before resetting the product, you may want to review the kinds of data that will be reset by browsing through the **Configure** page and associated tabs.

If the product configuration is reset, management access of the product may be lost until the network information is restored. The product must be offline before the configuration can be reset. See step 2 in "Configuring Ports" on page 31 for instructions on setting the product offline.

Note: Since the current IP address for the product may not match the factory default values, the Ethernet link between the product and the service processor may drop and not reset. Make sure you record the product's current IP address as you will want to enter that value in the **IP Address** field, under the **Configure** page, **Switch** or **Director** tab, and **Network** tab. See "Configuring Network Information" on page 45 for instructions.

Note: After you reset the product configuration, you should view the product information page as described in "Obtaining Product Information" on page 148. Save the product information page to a file or print the page to verify the changes you made and to identify the default values.

Clearing the System Error Light

The amber system error light indicator, shown on the **Switch** or **Director** tab view of the **View** page, simulates the system error light on the actual switch. When this indicator illuminates, an event has occurred requiring immediate attention, such as the failure of the system, power supply/fan, or port. For more information, see Table 5.

To clear the system error light, select **Operations** from the navigation panel. Select the **Switch** or **Director** tab as appropriate. Select the **Sys Err Light** tab to display the **System Error Light** tab view, which describes the current system error light state (Figure 44).

If the state of the system error light is **On**, click the **Clear Light** button to clear the error light.

If your change is successful, a message displays stating that your change has been successfully activated. You can refresh the web browser to verify that the change has been made.

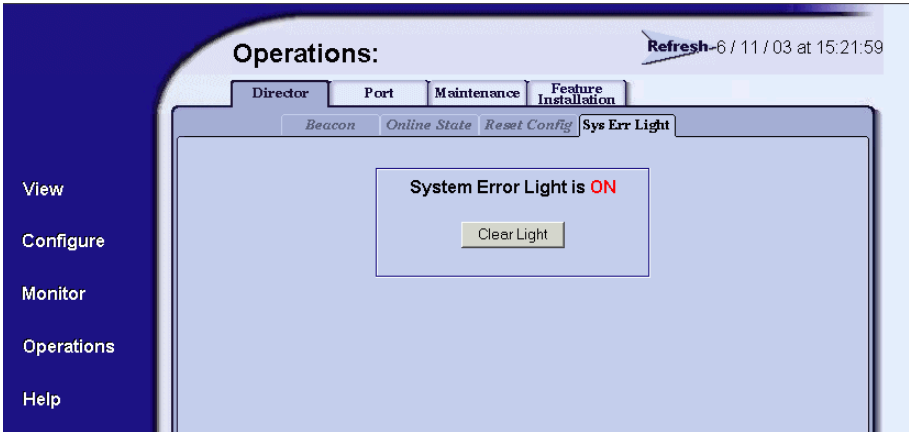


Figure 44: System Error Light

Set Individual Port Beaconing On or Off

Choose **Operations** from the navigation panel. Choose the **Port** tab and the **Beacon** tab; the **Beacon** tab view displays (Figure 45). Use this view to enable or disable beaconing for individual ports. Enabling beaconing helps you to locate a specific port for troubleshooting purposes by the use of flashing port LED. When there are multiple products stacked together, such as in a rack-mount cabinet, beaconing is useful to help locate a specific port by turning beaconing on for only that port.

The first column shows the port number, the second column contains the port name, as configured in the **Ports** tab view on the **Configure** page, and the third column contains check boxes to enable/disable beaconing.

A checked box indicates beaconing is active, an empty box indicates beaconing is not active for the port. To change the state click once inside the box. (A failed port cannot be set to beacon.) When finished, click **Activate** to enable the new configuration, or **Cancel** to return to the previous configuration. If your changes are successful, a message displays stating that your changes to the configuration have been successfully activated.

Note: For the Director 2/140, the ports are displayed through several pages in groups of 32. To configure the port beaconing, make sure you go through each set of ports.

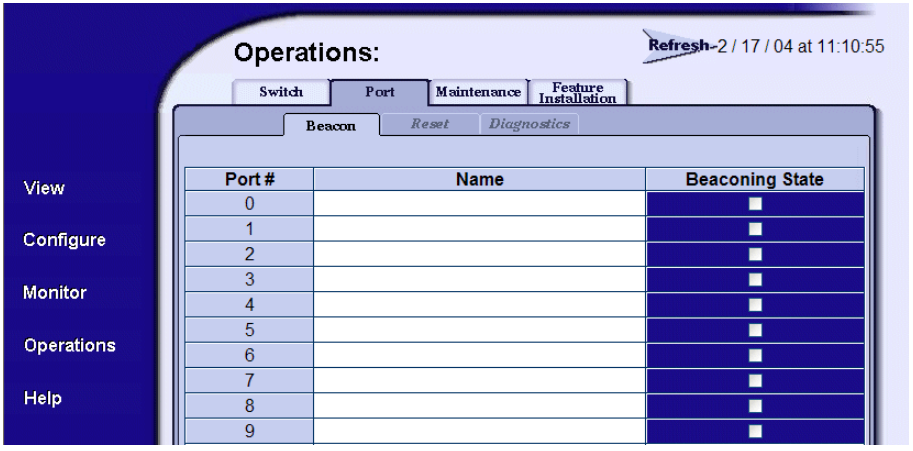


Figure 45: Setting individual port beaconing on or off

Resetting Ports

Choose **Operations** from the navigation panel. Choose the **Port** tab and the **Reset** tab; the **Reset** tab view displays (Figure 46). Use this page to reset ports. This action clears all statistics counters and disables port beaconing for the port. If a product is attached to the port and is online, this operation sends a link reset to the attached product; otherwise, this action disables port beaconing on the port. If the port is in a failed state, such as after failing a loopback test, the reset restores the port to an operational state and clears the service required (amber) LED. The reset does not affect other ports in the product.

To reset a port, click once in the box for that port's row, so that a check mark displays. When you have selected all ports to reset, click **Activate**. A message displays confirming that the operation has completed.

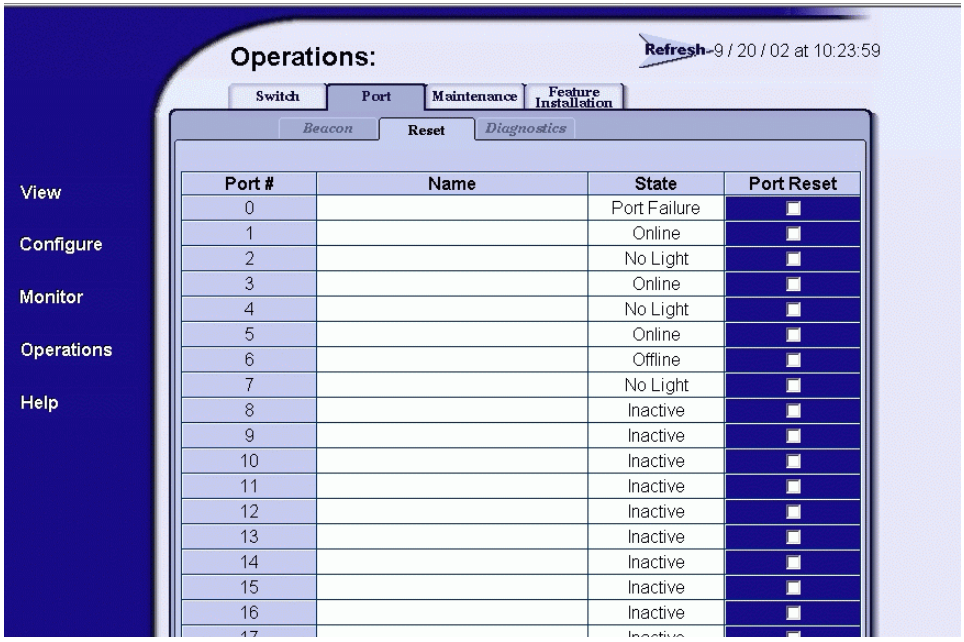


Figure 46: Resetting ports

Performing Diagnostics on Ports

Choose **Operations** from the navigation panel. Choose the **Port** tab and the **Diagnostics** tab; the **Diagnostics** tab view displays (Figure 47). Use this view to run either internal or external loopback diagnostic tests for any port. (Service personnel may request these tests to be conducted to aid in troubleshooting problems.)

- **Internal loopback test —** An internal loopback test checks internal port, serializer, and deserializer circuitry.
- **External loopback test —** An external loopback test checks all port circuitry, including fiber optic or copper components.

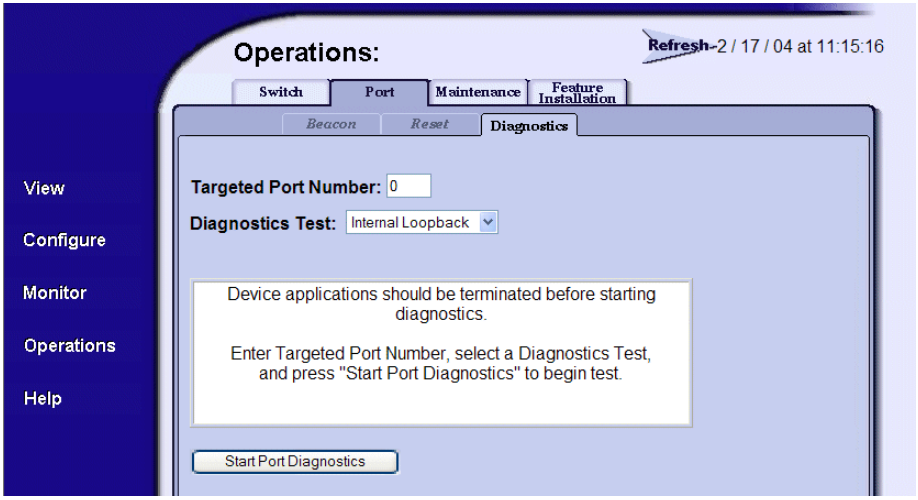


Figure 47: Performing diagnostics on ports

To run these tests, make sure that the administrator for any device attached to the ports quiesces Fibre Channel frame traffic through the product and sets the attached devices offline. A message will display in the status area to notify you that device applications should be terminated before starting diagnostics. However, since these tests disrupt port operation, make sure that there are no active nodes connected to the port(s) before starting a test. A loopback plug, furnished with the product, is required for the external loopback test.

Note: To identify port numbers on cards that you want to test, drag the mouse cursor across the cards in the **Unit view**. A label displays with the port number.

1. Enter a port number in the **Targeted Port Number** field.
2. Click the arrow on the **Diagnostic Test** drop-down list to display the available tests (**Internal Loopback** and **External Loopback**), then click a test to choose it.
3. Click **Start Port Diagnostics**. Port beaconing automatically initiates on the ports that you choose for loopback diagnostics (Figure 48). The test usually lasts 30 seconds.

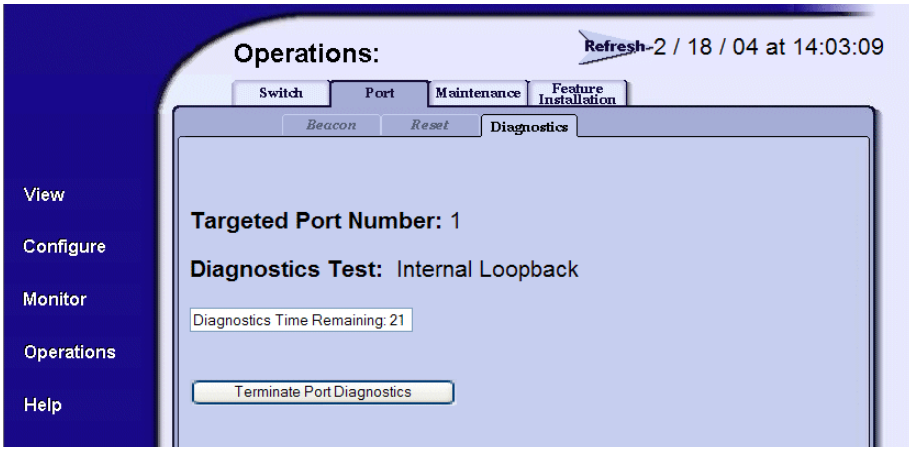


Figure 48: Diagnostics test in progress

Caution: When disconnecting a fiber optic cable to install an external loopback plug, make sure that you reconnect the cable to the same port after running the external loopback test.

The port's amber LED continues to beacon during the test. If running an internal loopback test, the green LED is off. If running an external loopback test, the green LED is on. Test status displays in the message window and the results display in the status area bar.

4. To stop a test, click **Terminate Port Diagnostics**. Beaconing automatically stops when the test completes or is canceled. If the port fails the test, the port's amber LED remains on.
5. Results display when the diagnostics finish or when you terminate the test. If errors occur, record all error information and refer to the product service documentation for problem isolation. See Figure 49 for an example of the screen when tests are completed.

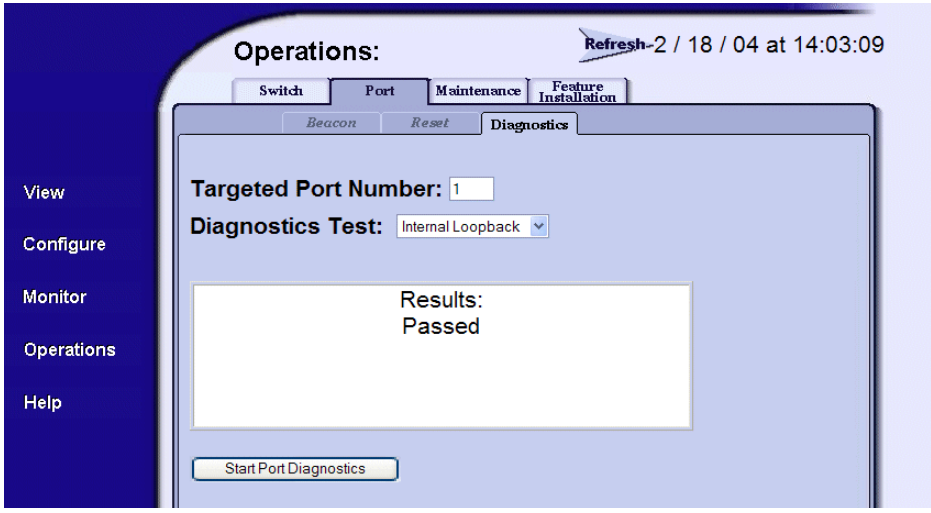


Figure 49: Completed diagnostics test

Retrieving Maintenance Information

If the operational firmware detects a critical error, the product automatically copies the contents of dynamic random access memory (DRAM) to a dump area in FLASH memory on the Control Processor (CTP) card; the CTP dump file contains this maintenance information. The CTP dump file will usually be requested by service personnel to aid in troubleshooting.

1. Choose **Operations** from the navigation panel.
2. Choose the **Maintenance** tab and the **Dump Retrieval** tab; the **Dump Retrieval** tab view displays (Figure 50).

Figure 50: Retrieving the CTP maintenance information

3. If no dump file is available, the message `Not Available` displays. If a dump file is available, follow the instructions shown in the tab view.
4. When you have accessed the **Save As** dialog box (Figure 51), choose **All Files** from the **Save as type:** field. When naming the file, add a "*.dmp*" extension to the filename.

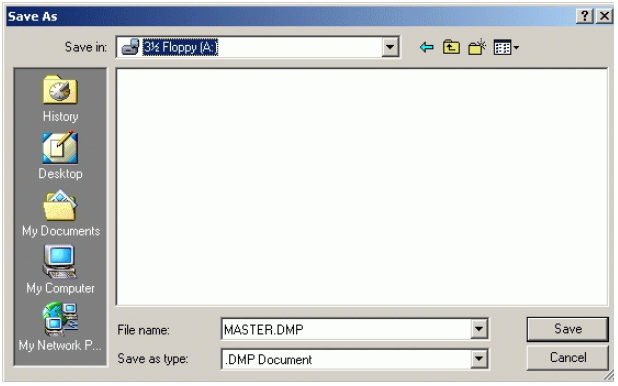


Figure 51: Choosing the location to save the CTP maintenance information

5. When the file is completely downloaded, the **Download Complete** screen displays. If you encounter any problems during this procedure, contact your service representative.

Obtaining Product Information

To obtain product information, choose the **Operations** page, then the **Maintenance** tab, and then choose **Product Info** tab. The **Product Info** tab view displays (Figure 52).

Figure 52: Obtaining product information

To view product information, choose the **Product Information** link in the right side of the table. A page with the following information is displayed:

Note: You may want to save this page to a file or print this page as the information may be requested by technical support to help resolve technical problems. (You may also want to enter a date in the file you save or on the printed page to note when the product information file was created.)

- Network Information (IP Address, Subnet Mask, Gateway Address)
- Identification Information
- Switch Information
- Fabric Parameters
- Port Configurations
- FRU List and Information
- SNMP Agent State
- Zoning Information

- Port Data
- Port Technology
- Port Login Data
- E_Port Status
- Switch Status
- Switch Configuration
- Installed Features
- Port Binding
- Switch Binding
- Fabric Binding
- Open Trunking Configuration
- Threshold Alerts
- Fabric Topology
- Fabric Node List

Upgrading Firmware

1. Choose the **Maintenance** tab from the **Operations** page, and then choose the **Firmware Upgrade** tab to upload and upgrade firmware. The **Firmware Upgrade** tab view displays (Figure 53).

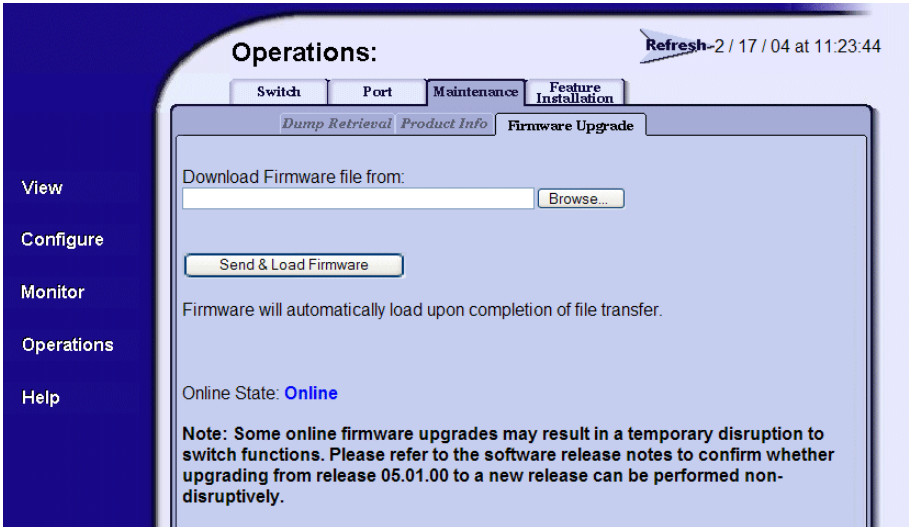


Figure 53: Upgrading firmware

The firmware version shipped with the product is provided on the documentation CD-ROM. Information about subsequent firmware versions is provided at HP's web site.

Detailed instructions on how to locate and download firmware are provided in the product's installation and service manuals.

Note: When adding a firmware version, follow all procedural information contained in the release notes that accompany the firmware version. That information supplements and supersedes information provided in this manual.

Note: Refer to the software release notes on whether the firmware upgrade can be done without causing a disruption as some upgrades may cause a temporary disruption to product function.

---

2. Type the drive path and name of the firmware file or click **Browse** to locate the file.
3. When the correct filename is in the **Download Firmware file from** field, click **Send & Load Firmware**. When the firmware has finished transferring, a message displays stating that the new firmware is being activated on the product and the product will be unavailable temporarily. You must reconnect to EWS after this period by logging back into EWS.

Note: You can verify the firmware was upgraded by viewing the **Unit Properties** tab under the **View** page. See "Viewing Unit Properties" on page 107.

Activating (Installing) Optional Features

This procedure is described in “Installing Feature Keys” on page 77.

Error Messages

This appendix lists and explains error messages for the Embedded Web Server. Any error numbers that are not listed are reserved for future use.

The message that is returned is a string that includes the error number and the text of the message.

Table 9: Embedded Web Server Messages

Message	Description	Action
Error 05: Busy	The switch cannot process any requests at this time.	Re-submit the request.
Error 08: Invalid Switch Name	The value entered for the switch name is invalid.	The name for the director or switch may contain 0—24 characters. Enter a name with 0—24 characters and resubmit. If spaces are used, enclose the name in quotation marks.
Error 09: Invalid Switch Description	The value entered for the switch description is invalid.	The description for the director or switch may contain 0—255 characters. Enter a description with 0—255 characters and resubmit. If spaces are used, enclose the description in quotation marks.
Error 10: Invalid Switch Location	The value entered for the switch location is invalid.	The location for the director or switch may contain 0—255 characters. Enter a location with 0—255 characters and resubmit. If spaces are used, enclose the location in quotation marks.

Table 9: Embedded Web Server Messages (Continued)

Message	Description	Action
Error 11: Invalid Switch Contact	The value entered for the switch contact is invalid.	The contact for the director or switch may contain 0—255 characters. Enter a contact with 0—255 characters and resubmit. If spaces are used, enclose the contact in quotation marks.
Error 13: Invalid Port Number	The value entered for the port number is invalid.	Enter a port number within the range supported by your director or switch. Valid values are: 0—15 for the Edge Switch 2/16 0—23 for the Edge Switch 2/24 0—31 for the Edge Switch 2/32 0—63 for the Director 2/64 0—127 and 132—143 for the Director 2/140
Error 14: Invalid Port Name	The value entered for the port name is invalid.	The port name for the individual port may contain 0—24 characters. Enter a name with 0—24 characters and resubmit. If spaces are used, enclose the name in quotation marks.
Error 15: Invalid BB Credit	The value entered for the buffer-to-buffer credit is invalid.	The buffer-to-buffer credit must be an integer in the range of 1—60.

Table 9: Embedded Web Server Messages (Continued)

Message	Description	Action
Error 16: Invalid R_A_TOV	The value entered for the resource allocation time-out value is invalid.	The R_A_TOV is entered in tenths of a second and must be entered as an integer in the range 10—1200 (1 second to 120 seconds). The R_A_TOV value must be larger than the E_D_TOV value. Check to be sure that all conditions are met and resubmit.
Error 15: Invalid BB Credit	The value entered for the buffer-to-buffer credit is invalid.	The buffer-to-buffer credit must be an integer in the range of 1—60.
Error 16: Invalid R_A_TOV	The value entered for the resource allocation time-out value is invalid.	The R_A_TOV is entered in tenths of a second and must be entered as an integer in the range 10—1200 (1 second to 120 seconds). The R_A_TOV value must be larger than the E_D_TOV value. Check to be sure that all conditions are met and resubmit.
Error 17: Invalid E_D_TOV	The value entered for the error detection time-out value is invalid.	The E_D_TOV is entered in tenths of a second and must be entered as an integer in the range 2—600 (0.2 second to 60 seconds). The E_D_TOV must be smaller than the R_A_TOV. Check to be sure that all conditions are met and resubmit.
Error 18: Invalid TOV	The E_D_TOV and R_A_TOV values are not compatible.	Enter a valid E_D_TOV / R_A_TOV combination. The E_D_TOV must be smaller than the R_A_TOV.

Table 9: Embedded Web Server Messages (Continued)

Message	Description	Action
Error 20: Invalid Preferred Domain ID	The value entered for the preferred domain ID for the director or switch is invalid.	The preferred domain ID must be an integer in the range 1—31. Enter an appropriate value and resubmit.
Error 21: Invalid Switch Priority	The value entered for the switch priority is invalid.	The switch priority entered for the director or switch must be one of the following: `principal`, `never principal`, or `default`. Enter an appropriate value and resubmit.
Error 29: Invalid Gateway Address	The value entered for the gateway address is invalid.	The new gateway address for the Ethernet interface must be entered in dotted decimal format (for example, 0.0.0.0). Enter an appropriate gateway address and resubmit.
Error 30: Invalid IP Address	The value entered for the IP Address is invalid.	The new IP address for the Ethernet interface must be entered in dotted decimal format (for example, 10.0.0.0). Enter an appropriate IP address and resubmit.
Error 31: Invalid Subnet Mask	The value entered for the subnet mask is invalid.	The new subnet mask for the Ethernet interface must be entered in dotted decimal format (for example,. 255.0.0.0). Enter an appropriate subnet mask and resubmit.

Table 9: Embedded Web Server Messages (Continued)

Message	Description	Action
Error 32: Invalid SNMP Community Name	The value entered for the SNMP community name is invalid.	The community name must not exceed 32 characters in length. Duplicate community names are allowed, but corresponding write authorizations must match. Enter an appropriate SNMP community name and resubmit.
Error 33: Invalid SNMP Trap Address	The value entered for the SNMP trap address is invalid.	The new SNMP trap address for the SNMP interface must be entered in dotted decimal format (for example, 10.0.0.0). Enter an appropriate SNMP trap address and resubmit.
Error 34: Duplicate Community Names Require Identical Write Authorization	Two or more community names have been recognized as being identical, but their corresponding write authorizations are not identical.	Enter unique SNMP community names or force write authorizations for duplicate community names to be identical and resubmit.
Error 37: Invalid Month	The value of the month entered for the new system date is invalid.	The format of the date parameter must be mm:dd:yyyy or mm/dd/yyyy. The month must contain an integer in the range 01—12. Enter an appropriate date and resubmit.
Error 38: Invalid Day	The value of the day entered for the new system date is invalid.	The format of the date parameter must be mm:dd:yyyy or mm/dd/yyyy. The day must contain an integer in the range 01—31. Enter an appropriate date and resubmit.

Table 9: Embedded Web Server Messages (Continued)

Message	Description	Action
Error 39: Invalid Year	The value of the year entered for the new system date is invalid.	The format of the date parameter must be mm:dd:yyyy or mm/dd/yyyy. The year must contain an integer greater than 1980. Enter an appropriate date and resubmit.
Error 40: Invalid Hour	The value of the hour entered for the new system time is invalid.	The format of the time parameter must be hh:mm:ss. The hour can contain an integer in the range 00—23. Enter an appropriate time and resubmit.
Error 41: Invalid Minute	The value of the minute entered for the new system time is invalid.	The format of the time parameter must be hh:mm:ss. The minute can contain an integer in the range 00—59. Enter an appropriate time and resubmit.
Error 42: Invalid Second	The value of the second entered for the new system time is invalid.	The format of the time parameter must be hh:mm:ss. The second can contain an integer in the range 00—59. Enter an appropriate time and resubmit.
Error 44: Max SNMP Communities Defined	A new SNMP community may not be defined without removing an existing community from the list.	A total of 6 communities may be defined for SNMP. A new community can be added only after a current community is removed. Make the appropriate changes and resubmit.
Error 45: Not Allowed While Switch Online	The entered command requires that the director or switch be set offline.	Set the switch offline and resubmit the command.

Table 9: Embedded Web Server Messages (Continued)

Message	Description	Action
Error 55: Invalid Zone Name	The value entered for the zone name is invalid.	The zone name must be unique and contain 1—64 characters.
Error 57: Duplicate Zone	Two or more zone names in the zone set are identical.	All zone names must be unique. Make the appropriate changes and resubmit.
Error 59: Zone Name in Use	Two or more zone names in the zone set are identical.	All zone names must be unique. Make the appropriate changes and resubmit.
Error 60: Invalid Number of Zone Members	The entered command tried to add more zone members than the zone can hold.	Reduce the number of zone members in the zone and resubmit the command.
Error 61: Invalid Zone Member Type	A zone member was entered that is neither a WWN nor a Domain, Port pair.	Zone members must be expressed in WWN format or as a Domain, Port pair. Make the appropriate changes and resubmit.
Error 62: Invalid Zone Set Name	The value entered for the zone set name is invalid.	The zone set name must be contain 1—64 characters. Make the appropriate changes to the zone set name and resubmit.
Error 69: Duplicate Port Name	Two or more port names are identical.	Port names must be unique. Make appropriate changes and resubmit.
Error 70: Invalid FRU Type	The specified FRU does not exist on this product	Consult the installation/service manual for this product to find appropriate FRU names.
Error 71: FRU Not Installed	The specified FRU is not installed.	Consult the installation/service manual for this product for appropriate action.

Table 9: Embedded Web Server Messages (Continued)

Message	Description	Action
Error 72: No Backup FRU	The FRU cannot be swapped because a backup FRU is not installed.	Insert a backup FRU and resubmit the request or consult the installation or service manual for this product for appropriate action.
Error 73: Port Not Installed	The port specified is not installed on this product.	Consult the installation/service manual on installing a port optic.
Error 74: Invalid Number of Zones	The specified zone set contains less than one zone or more than the maximum number of zones allowed for this product.	A zone set must contain at least one zone to be considered valid. Add or remove zones accordingly to meet specified requirements.
Error 75: Invalid Zone Set Size	The zone set entered exceeds switch NVRAM limitations.	Reduce the size of the zone set to meet specified requirements. This can be a reduction in the number of zones in the zone set, a reduction of members in a zone, or a reduction of zone name lengths.
Error 76: Invalid Number of Unique Zone Members	The zone entered contains more than the maximum number of zone members allowed per zone set for this product.	Reduce the number of members in one or more zones and resubmit the command.
Error 77: Not Allowed While Port Is Failed	The port selected is in a failed or inactive state, or is in need of service.	Consult the installation/service manual for appropriate action.
Error 78: System Error Light On	This unit is not able to beacon because the system error light is on.	You must clear the system error light before unit beaconing may be enabled. Consult the installation/service manual for appropriate action.

Table 9: Embedded Web Server Messages (Continued)

Message	Description	Action
Error 79: FRU Failed	The specified FRU has failed.	Consult the installation/service manual for appropriate action.
Error 81: Default Zone Enabled	The request cannot be completed because the default zone is enabled	Disable the default zone and resubmit the command.
Error 82: Invalid Interop Mode	The value entered for the interoperability mode is not valid.	The interoperability mode for the director or switch must be mcdata (Homogenous Fabric) or open (Open Fabric 1.0). Make the appropriate changes and resubmit the command.
Error 83: Not Allowed in Open Fabric Mode	This request cannot be completed while this switch is operating in Open Fabric 1.0 mode.	Configure the interop mode to Homogenous Fabric mode.
Error 88: Invalid Feature Key Length	The feature key installed is longer than the maximum length allowed.	Be sure that the key has been entered correctly and resubmit. Contact your sales representative with any further problems.
Error 89: Not Allowed in S/390 Mode Without the SANtegrity Feature	Cannot configure port types in S/390 mode (FICON management style in HAFM) without installing SANtegrity.	This command is only supported when the switch is in Open Systems mode (Open Systems management style in HAFM) or in S/390 mode (FICON management style in HAFM) with SANtegrity.
Error 90: Invalid Port Type	The port type configured is invalid.	A port may be configured to be an eport, gport, or fport. Be sure the port is configured appropriately and resubmit the command.

Table 9: Embedded Web Server Messages (Continued)

Message	Description	Action
Error 91: E_Port Type Configured	Ports are not allowed to be configured as E_Ports in S/390 mode (FICON management style in HAFM).	Configure the port as either an fport or gport and resubmit the command.
Error 92: Not Allowed While Port Is Unblocked	The port must be blocked to complete this request.	Block the port and resubmit the command.
Error 93: Not Allowed While FICON MS Is Installed	This request cannot be completed because FICON Management Server is installed.	This operation is not supported. No action necessary.
Error 94: Invalid Feature Combination	The features requested cannot be installed at the same time on one director or switch.	Contact your sales representative.
Error 99: Preferred Domain ID Cannot Be Zero	This product cannot be configured to have a preferred domain ID equal to zero (0).	Ensure that the ID is expressed as an integer in the range 1—31 and resubmit.
Error 101: Command Not Supported on This Product	This product does not support the requested command.	Command not supported. No action necessary.
Error 102: Switch Not Operational	The request cannot be completed because the switch is not operational.	Consult the installation/service manual and contact your service representative.
Error 103: Port Diagnostic In Progress	The request cannot be completed because a port diagnostic is running.	Wait for the diagnostic to complete.
Error 104: System Diagnostic In Progress	The request cannot be completed because a system diagnostic is running.	Wait for the diagnostic to complete.
Error 105: Max Threshold Definitions Reached	The maximum number of total threshold alerts has already been reached.	Remove a threshold alert before adding the new threshold alert. A total of 16 counter and throughput threshold alerts is allowed.

Table 9: Embedded Web Server Messages (Continued)

Message	Description	Action
Error 106: Invalid Threshold Scope	The scope of a threshold alert is not set to a valid state before the user activates an alert.	Set the scope of the threshold alert, then try to activate the alert.
Error 107: Invalid Threshold State	The scope of a threshold alert must be set before the user activates an alert.	Set the scope of the threshold alert, then try to activate the alert.
Error 108: Invalid TTA Type	The type of the throughput threshold alert (TTA) has not been set.	Set the type of the TTA, then try to activate the alert.
Error 109: Invalid CTA Type	The type of the counter threshold alert has not been set.	Set the type of the CTA, then try to activate the alert.
Error 110: Invalid Percent Utilization	The type of the throughput threshold alert has not been set.	Set the type of the TTA, then try to activate the alert.
Error 111: Invalid Threshold Type	The type of the threshold alert is not valid.	Configure the type of the throughput threshold alert to one of the types found in the enumerated table for TTAs.
Error 112: No Threshold Definition Given	The threshold value for the alert was not configured before the user attempted to activate the alert.	Set the threshold value, then try to activate the alert.
Error 115: Invalid Switch Speed	The request cannot be completed because the switch is not capable of operating at the configured speed.	Consult the installation/service manual to determine the speed capabilities of your product.
Error 116: Switch Not Capable of 2 Gb/sec	The request cannot be completed because the switch is not capable of operating at 2 Gb/s.	Consult the installation/service manual to determine the speed capabilities of your product.

Table 9: Embedded Web Server Messages (Continued)

Message	Description	Action
Error 117: Port Speeds Cannot be Set at Higher Data Rate than Switch Speed	This request cannot be completed because the requested port speed is faster than the currently-configured switch speed.	The switch speed should first be configured to accommodate changes in the configured port speed. The ports cannot operate at a faster rate than the switch, itself. Update the switch speed and resubmit the request.
Error 118: Invalid Port Speed	This request cannot be completed because the requested port speed is not recognized for this product.	Port speeds may be set to 1 Gb/s or 2 Gb/s. Update the port speed and resubmit the request.
Error 119: Switch Speed Not 2 Gb/sec	This request cannot be completed because the switch speed has not been set to 2 Gb/s.	The switch speed must be set to 2 Gb/s in order to accommodate a port speed of 2 Gb/s. Update the switch speed and resubmit the request.
Error 134: Invalid Membership List	Generic message to indicate a problem in either the switch binding or fabric binding membership list.	Be sure that the membership list submitted does not isolate a switch already in the fabric. If this is not the case, the user needs to be aware of all fabric security rules and make sure that the list submitted adheres appropriately.
Error 135: Invalid Number of Fabric Membership List Entries	The number of fabric members submitted exceeds the maximum allowable entries of 31.	The number of entries in the fabric membership list is limited to the total number of domain ID's available to the fabric. Make sure that the list (including the managed switch) contains no more than 31 entries.

Table 9: Embedded Web Server Messages (Continued)

Message	Description	Action
Error 136: Invalid Number of Switch Membership List Entries	The number of switch members submitted exceeds the maximum allowable entries of 256.	The number of entries in the switch membership list is limited to 256. Make sure that the list (including the managed switch) contains no more than 256 entries.
Error 137: Invalid Fabric Binding State	The fabric binding state submitted is not recognized by the CLI.	The fabric binding state must be set to either `inactive` or `restrict`.
Error 138: Invalid Switch Binding State	The switch binding state submitted is not recognized by the system.	The switch binding state must be set to one of the following: `disable`, `erestrict`, `frestrict`, or `allrestrict`.
Error 139: Insistent Domain IDs Must Be Enabled When Fabric Binding Active	The user attempted to disable insistent domain ID's while fabric binding was active.	Insistent domain IDs must remain enabled while fabric binding is active. If fabric binding is set to inactive, the insistent domain ID state may be changed. It should be noted, however, that this can be disruptive to the fabric.
Error 140: Invalid Insistent Domain ID State	The request cannot be completed because an invalid insistent domain ID state has been submitted.	The insistent domain ID state must be set to either enable or disable.
Error 141: Invalid Enterprise Fabric Mode	The request cannot be completed because an invalid enterprise fabric mode has been submitted.	The enterprise fabric mode must be set to either activate or deactivate.
Error 142: Invalid Domain RSCN State	The request cannot be completed because an invalid domain RSCN state has been submitted.	The domain RSCN state must be set to either enable or disable.

Table 9: Embedded Web Server Messages (Continued)

Message	Description	Action
Error 143: Domain RSCNs Must Be Enabled When Enterprise Fabric Mode Active	The user attempted to disable domain RSCNs while enterprise fabric mode was active.	Domain RSCNs must remain enabled while the enterprise fabric mode is active. If enterprise fabric mode is set to inactive, the domain RSCN state may be changed. It should be noted, however, that this can be disruptive to the fabric.
Error 144: The SANtegrity Feature Has Not Been Installed	The user attempted to activate a change to the fabric security configuration without first installing the SANtegrity Binding feature key.	If this key has not been installed, contact your sales representative.
Error 146: Fabric Binding May Not Be Deactivated While Enterprise Fabric Mode Active	The user attempted to deactivate fabric binding while enterprise fabric mode was active.	Fabric binding must be active while operating in enterprise fabric mode. The fabric binding state may be changed if enterprise fabric mode is deactivated. It should be noted, however, that this can be disruptive to the fabric.
Error 148: Not Allowed While Switch Offline	The switch must be online to complete this request.	Change the state of the switch to ONLINE and resubmit the request.
Error 149: Not Allowed While Enterprise Fabric Mode Enabled and Switch Active	The request cannot be completed while the switch is online and enterprise fabric mode is Active.	This operation will be valid if the switch state is set to offline and enterprise fabric mode to inactive. It should be noted, however, that this can be disruptive to the fabric.
Error 151: Invalid Open Systems Management Server State	The request cannot be completed because the OSMS state submitted is invalid.	The OSMS state may be set to either enable or disable.

Table 9: Embedded Web Server Messages (Continued)

Message	Description	Action
Error 152: Invalid FICON Management Server State	The request cannot be completed because the FICON MS state submitted is invalid.	The FICON MS state may be set to either enable or disable.
Error 153: Feature Key Not Installed	The request cannot be completed because the required feature key has not been installed to the firmware.	Contact your sales representative.
Error 154: Invalid Membership List WWN	The request cannot be completed because the WWN does not exist in the switch binding membership list.	Make sure that the WWN deleted matches the WWN in the switch membership list. Make appropriate changes and resubmit the request.
Error 155: Cannot Remove Active Member From List	This member cannot be removed from the fabric security list because it is currently logged in.	Fabric security rules prohibit any device or switch from being isolated from the fabric via a membership list change. If it is truly the intention of the user to remove the device in question from the membership list, then there are several approaches to take. This request may be completed most non-disruptively by blocking the port (or physically removing the device from the managed switch) to which this device is attached and resubmitting the request.
Error 156: Cannot Disable Fabric Binding while Switch is Online	The switch must be offline and fabric binding must be inactive before this feature can be disabled.	Deactivating this feature can be disruptive to Fabric operations. Take the switch offline and deactivate fabric binding before disabling this feature.

Table 9: Embedded Web Server Messages (Continued)

Message	Description	Action
Error 157: Access Control List is Disabled	The switch must be offline and Fabric Binding must be inactive before this feature can be disabled.	Deactivating this feature can be disruptive to Fabric operations. Take the switch offline and deactivate fabric binding before disabling this feature.
Error 158: Invalid IP Access Control List Pair	The pair of IP addresses are invalid and cannot be added to the list.	Make sure the IP addresses are valid and the first IP is lower than the second
Error 159: Invalid IP Access Control List Pairs Count Value	The list being activated has an invalid number of IP pairs.	Make sure there is at least one IP address in the Access Control List.
Error 160: Management Client IP Not Included In IP Access Control List	The management interface IP address is not in the list.	The management IP must be in the list or the current connection would be lost.
Error 161: SANtegrity Authentication feature key must be uninstalled	The operation cannot be completed with the SANtegrity Authentication key installed.	Remove the SANtegrity Authentication feature key.
Error 162: List is full	There is no more room for new entries in the list.	Remove a different entry and try again.
Error 163: FICON MS feature key must be installed	The command is not available without the FICON MS feature key.	Install the FICON MS feature key.
Error 164: FICON CUP Zoning feature key must be uninstalled	The operation cannot be completed with the FICON CUP Zoning key installed.	Remove the FICON CUP Zoning feature key.
Error 165: CUP Zoning feature key must be installed	The command is not available without the FICON CUP Zoning feature key	Install the FICON CUP zoning feature key.
Error 166: CUP Zoning feature must be enabled	The command cannot be completed with the CUP Zoning feature enabled	Enable FICON CUP Zoning.
Error 167: Diagnostics can not be run on inactive port	The port is in the inactive state and diagnostics can't be run.	The port state must change out of the inactive state.

Table 9: Embedded Web Server Messages (Continued)

Message	Description	Action
Error 168: Duplicate member in the list	The member is already in the list.	Duplicate members are not allowed in the list.
Error 169: CNT support in is an incorrect enabled state	Computer Network Technology (CNT) support is in the wrong state.	The enabled state for CNT support must be changed.
Error 170: Duplicate IP Address pair in the Access Control List	Duplicate IP address pairs are not allowed in the Access Control List.	This command is redundant, the member already exists in the list.
Error 171: Invalid username	The username is invalid.	Enter a unique username using only the allowed characters and proper length.
Error 172: Invalid list size	The number of entries in the list is invalid.	Make sure the list has at least one entry.
Error 173: Invalid value	The value being entered is invalid.	Enter a valid value.
Error 174: Invalid list data	The list data is invalid.	Correct the list to make it a valid list.
Error 175: Invalid list index (the user should not see this error)	The index in the list is incorrect.	Correct the index.
Error 176: Entry not found in the list	The desired entry in the list does not exist.	Make sure the desired entry is in the list and it is being typed correctly.
Error 177: Cannot remove the last user with Administrator rights	At least one Administrator user must exist for each management interface.	Add a new Administrator and then try again.
Error 178: Invalid password	The entered password is invalid.	Enter a password using valid characters and a proper length.
Error 179: Insistent Domain IDs must be enabled	To complete this command, Insistent Domain IDs must be enabled.	Enabled Insistent Domain IDs.
Error 180: Too many authentication management users	Only 25 management users can be added to the user database.	Remove other management users in order to make room for a new one.

Table 9: Embedded Web Server Messages (Continued)

Message	Description	Action
Error 181: Preferred path must be disabled	The Preferred Path feature must be disabled.	Disable the Preferred Path feature.
Error 182: Source port must be different than the exit port	The source and exit ports cannot be the same.	Configure a preferred path with different source and exit ports.
Error 201: Change Authorization Request Failed	The switch did not accept the request to make a change to NVRAM.	Be sure all parameters have been entered correctly and resubmit. Contact your service representative with further problems.
Error 202: Invalid Change Authorization ID	The switch will not accept a change request from this particular client.	Be sure all parameters have been entered correctly and resubmit. Contact your service representative with further problems.
Error 203: Another Client Has Change Authorization	Another user is currently making changes to this switch.	Be sure all parameters have been entered correctly and resubmit.
Error 207: Change Request Failed	The switch did not accept the request.	Be sure all parameters have been entered correctly and resubmit. Contact your service representative with further problems.
Error 208: Change Request Timed Out	Authorization time to make NVRAM changes has expired.	Be sure all parameters have been entered correctly and resubmit. Contact your service representative with further problems.
Error 209: Change Request Aborted	The switch did not accept the request.	Be sure all parameters have been entered correctly and resubmit. Contact your service representative with further problems.

Table 9: Embedded Web Server Messages (Continued)

Message	Description	Action
Error 210: Busy Processing Another Request	A different switch in the Fabric was busy processing another request and could not complete the command.	Be sure all parameters have been entered correctly and resubmit. Contact your service representative with continued problems.
Error 211: Duplicate Zone	Two or more zone names in the local zone set are identical.	All zone names must be unique. Make the appropriate changes and resubmit.
Error 212: Duplicate Zone Member	A member was added that already exists in the zone.	No action necessary.
Error 213: Number of Zones Is Zero	You are attempting to activate and empty zone set.	The zone set must have at least one zone to be considered valid. Add a valid zone to the zone set and resubmit.
Error 214: A Zone Contains Zero Members	You are attempting to activate a zone set that contains at least one zone with zero members.	Each zone in the zone set must contain at least one member. Add a valid member to the empty zone and resubmit.
Error 215: Zone Set Size Exceeded	The local work area zone set has outgrown the size limitations imposed by the Command Line Interface.	Reduce the size of the zone set to meet CLI requirements. This can be a reduction in the number of zones in the zone set, a reduction of members in a zone, or a reduction of zone name lengths.

Table 9: Embedded Web Server Messages (Continued)

Message	Description	Action
Error 218: Invalid Port Number	The value entered for the port number is invalid	Enter a port number within the range supported by your director or switch. Valid values are: 0—15 for the Edge Switch 2/16 0—23 for the Edge Switch 2/24 0—31 for the Edge Switch 2/32 0—63 for the Director 2/64 0—127 and 132—143 for the Director 2/140
Error 219: Invalid Port Type	The port type configured is invalid.	A port may be configured to be an eport, gport, or fport. Be sure the port is configured appropriately and resubmit the command. On the Edge Switch 2/24 only, fxport and gxport types are also supported.
Error 222: Invalid SNMP Community Index	The value entered for the SNMP community index is invalid.	The SNMP community index must be an integer in the range 1—6. Make the appropriate changes and resubmit the command.
Error 223: Unknown Error	The switch did not accept the request	Contact your service representative.
Error 224: Invalid Argument	One or more parameters are invalid for this command.	For the appropriate parameters, see the section of the manual that corresponds to the attempted command.

Table 9: Embedded Web Server Messages (Continued)

Message	Description	Action
Error 225: Argument Does Not Contain All USASCII Characters	The argument contains non-USASCII characters.	For the appropriate parameters, see the section of the manual that corresponds to the attempted command.
Error 226: Argument Is Too Long	One or more parameters are invalid for this command.	For the appropriate parameters, see the section of the manual that corresponds to the attempted command.
Error 227: Invalid SNMP Community Name	The value entered for the SNMP community name is invalid	The community name must not exceed 32 characters in length. Duplicate community names are allowed, but corresponding write authorizations must match. Enter an appropriate SNMP community name and resubmit.
Error 228: Invalid Write Authorization Argument	The write authorization parameter does not contain a valid value.	Parameters must be typed exactly to specification to be recognized correctly.
Error 229: Invalid UDP Port Number	The `udpPortNum` parameter does not contain a valid value.	Parameters must be typed exactly to specification to be recognized correctly by the system.
Error 230: Invalid WWN	The `wwn` parameter does not contain a valid value.	For the appropriate parameters, see the section of the manual that corresponds to the attempted command.
Error 231: Invalid Port number	The `portNum` parameter does not contain a valid value.	For the appropriate parameters, see the section of the manual that corresponds to the attempted command.

Table 9: Embedded Web Server Messages (Continued)

Message	Description	Action
Error 232: Invalid Domain ID	The `domainID` parameter does not contain a valid value.	For the appropriate parameters, see the section of the manual that corresponds to the attempted command.
Error 233: Invalid Member	The zone member added is not valid.	For the appropriate parameters, see the section of the manual that corresponds to the attempted command.
Error 234: Invalid Command	The system cannot associate an action with the submitted command. The command may be misspelled, required parameters may be missing, or the request may not be applicable.	Consult the documentation for the command to be sure this command was entered correctly, all parameters are valid and present, and that the syntax is correct.
Error 235: Unrecognized Command	Cannot recognize the command and cannot perform the help '?' command as requested.	The entered command is misspelled, or the prompt is not positioned at the right place. For the appropriate syntax, see the section of the manual that corresponds to the attempted command.
Error 236: Ambiguous Command	Cannot recognize the command issued.	The command cannot be interpreted because a unique match cannot be identified. For the appropriate syntax, see the section of the manual that corresponds to the attempted command. Enter the complete command and resubmit.
Error 237: Invalid Zoning Database	There was an unidentifiable problem in the local zone set work area.	Verify all parameters are entered correctly and resubmit. Otherwise, the pending zone set should be cleared and reconstructed.

Table 9: Embedded Web Server Messages (Continued)

Message	Description	Action
Error 238: Invalid Feature Key	The feature key entered is invalid.	Verify that the feature key was entered correctly and resubmit. Contact your service representative with further difficulties.
Error 239: Fabric binding entry not found	The user requested to remove a fabric binding entry that is not in the pending fabric membership list.	Verify that the correct entry (both WWN and Domain ID) is being requested for removal from the list and resubmit the request.
Error 240: Duplicate fabric binding member	The user requested to add an entry to the fabric binding list that is already a member of the list.	Verify that the correct entry (both **WWN** and **Domain ID**) is being requested for addition to the list and resubmit the request.
Error 241: Comma-delimited mode must be active	Comma-delimited mode must be active to execute this command	Some commands require that comma-delimited mode be active (for example, `show.nameserverExt`). Enable comma-delimited mode and re-issue the command.
Error 242: Open trunking threshold % value must be 0—99	An invalid threshold percentage has been entered.	The Open trunking threshold must be in the range 0—99. Make sure all values are valid and resubmit the request.
Error 243: Not allowed while S/390 Mode is Enabled	This operation is not allowed while S/390 mode (FICON management style in HAFM) is enabled.	This command is not valid for the S/390 environment (FICON management style in HAFM).
Error 244: Not allowed while Enterprise Fabric Mode is Active and Switch is Online	This operation is not allowed while the switch is in Enterprise Fabric mode and the switch is online.	Make sure Enterprise Fabric mode is not enabled and the switch is offline.

Table 9: Embedded Web Server Messages (Continued)

Message	Description	Action
Error 245: Invalid increment value	The increment value specified is not between 1 and 70560.	Make sure the increment value given is between 1 and 70560.
Error 246: Invalid interval value	The interval value specified is not between 5 and 70560 minutes.	Make sure the increment value given is between 5 and 70560 minutes.
Error 247: Invalid counter number	The counter specified is not a valid number.	Use the table shown by the command `perf.counterThreshAlerts.showStatisticsTable` to find a valid counter value.
Error 248: A counter must be assigned to this threshold alert	A counter must be assigned to an alert before it is enabled.	Use the `perf.counterThreshAlerts.setCounter` command to set a counter before the alert is enabled.
Error 249: At least one port or port type must be added to this threshold alert	A port or port type must be assigned to an alert before it is enabled.	Use the `perf.counterThreshAlerts.addPort` command to add a port before the alert is enabled.
Error 250: Invalid counter threshold alert name	The name specified for the alert is not valid.	A counter threshold alert with the specified name does not exist.
Error 251: The threshold alert must be disabled	The counter threshold alert to be modified/deleted is already enabled.	Disable the threshold alert and then try the command again.
Error 252: Not Allowed While the Pending Fabric Binding State is Set to Inactive	The pending fabric binding set must be set to `Restrict` in order to edit the pending fabric binding list.	Set the pending fabric binding state to `Restrict`.

Table 9: Embedded Web Server Messages (Continued)

Message	Description	Action
Error 253: Cannot Remove a Member Currently Interacting with the Fabric	Current members of the fabric must be included in the Fabric Binding List.	Do not remove active fabric members from the pending Fabric Binding List.
Error 254: A utilization type must be assigned to this threshold alert	A utilization type must be set before activating this threshold alert.	Add a utilization type and then the threshold alert can be activated.
Error 255: Invalid throughput threshold alert name	The name of the threshold alert is incorrect.	Either the name does not exist, or the new name cannot be used because it is illegal or a duplicate.
Error 256: Invalid utilization type number	The utilization type number does not exist.	Select a valid utilization type number.
Error 257: Invalid utilization percentage value	The utilization percentage value is out of range.	Select a valid utilization percentage value.
Error 258: Invalid duration value	The duration value in minutes is out of range.	Select a valid duration value.
Error 259: Invalid threshold alert name	The name of the threshold alert is incorrect.	The threshold alert name does not exist.
Error 260: Not Allowed while SANtegrity feature is not installed on any remote switch	All switches in the fabric must have the SANtegrity feature key installed.	Install the SANtegrity feature key on all switches in the fabric.
Error 261: No Attached Members Exist	There are no members attached to the switch.	Check all connections and make sure attached devices are present.
Error 262: All Attached Members are in the Membership List	All attached fabric members are already in the membership list.	This action is redundant, all members are already in the list.
Error 263: The SANtegrity Authentication feature key is not installed	The SANtegrity Authentication feature key is not installed.	Install the SANtegrity Authentication feature key.

Table 9: Embedded Web Server Messages (Continued)

Message	Description	Action
Error 264: The Preferred Path feature key is not installed	The preferred path feature key must be installed.	Install the preferred path feature key.
Error 265: Duplicate threshold alert name	The desired name for the threshold alert is already in use.	Use a different name for the threshold alert.
Error 266: Attached members cannot be added while fabric is building	Attached members cannot be added while the fabric is building.	The fabric is still building, wait a couple of seconds until it is complete.

Index

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

Z